Universidade Federal do Paraná

Adi Nascimento Marcondes

Um Esquema de Autenticação Resistente à Ataques de Repetição de Identidades em Redes Heterogêneas

Curitiba PR
2016

Adi Nascimento Marcondes

Um Esquema de Autenticação Resistente à Ataques de Repetição de Identidades em Redes Heterogêneas

Dissertação apresentada como requisito parcial à obtenção do grau de Mestre em Informática no Programa de Pós-Graduação em Informática, setor de Ciências Exatas, da Universidade Federal do Paraná.

Área de concentração: *Ciência da Computação*.

Orientador: Aldri Luiz dos Santos.

Co-orientador: Michele Nogueira Lima.

Curitiba PR
2016

Dados Internacionais de Catalogação na Publicação (CIP)
Elaborado por: Sônia Magalhães
Bibliotecária CRB 9/1191

Marcondes, Adi Nascimento
M321 Um esquema de autenticação resistente á ataques de repetição de
2016 identidades em redes heterogêneas / Adi Nascimento Marcondes ; orientador ; Aldri Luiz dos Santos ; co-orientadora, Michele Nogueira Lima. – 2016.
48 f. ; 30 cm

Dissertação (mestrado) – Universidade Federal do Paraná, Curitiba, 2016
Bibliografia: f. 47-50

1. Rede locais sem fio. 2. Redes heterogêneas. 3. Informática. I. Santos, Aldri Luiz dos. II. Lima, Michele Nogueira. III. Universidade Federal do Paraná. Programa de Pós-Graduação de Informática. IV. Título.

CDD 20. ed. – 004.68

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO PARANÁ
PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO
Setor CIÊNCIAS EXATAS
Programa de Pós Graduação em INFORMÁTICA
Código CAPES: 40001016034P5

TERMO DE APROVAÇÃO

Os membros da Banca Examinadora designada pelo Colegiado do Programa de Pós-Graduação em INFORMÁTICA da Universidade Federal do Paraná foram convocados para realizar a arguição da Dissertação de Mestrado de **ADI NASCIMENTO MARCONDES**, intitulada: "**Um esquema de autenticação resistente a ataques de repetição de identidades em redes heterogêneas**", após terem inquirido o aluno e realizado a avaliação do trabalho, são de parecer pela sua APROVAÇÃO.

Curitiba, 25 de Agosto de 2016.

Aldri Luiz dos Santos
Prof ALDRI LUIZ DOS SANTOS
Presidente da Banca Examinadora (UFPR)

Michele Nogueira Lima
Prof MICHELE NOGUEIRA LIMA
Coorientador - Avaliador Interno (UFPR)

Prof ALTAIR OLIVO SANTIN
Avaliador Externo (PUC/PR)

Kleber Vieira Cardoso
Prof KLEBER VIEIRA CARDOSO
Avaliador Externo (UFG)

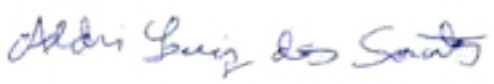
Ministério da Educação
Universidade Federal do Paraná
Programa de Pós-Graduação em Informática

DECLARAÇÃO

Curitiba, 25 de Novembro de 2016.

Ao programa de Pós-Graduação em Informática da UFPR, declaro que o aluno **Adi Nascimento Marcondes**, matriculado no curso de mestrado realizou as correções sugeridas pela banca.

Atenciosamente,



Prof. Dr. Aldri Luiz dos Santos

Esta dissertação é dedicada a minha família, aos amigos, aos colegas do grupo de pesquisa NR2 e a comunidade acadêmica.

Agradecimentos

Gostaria de agradecer primeiramente à Deus por me ajudar em tudo e minha família que meu deu apoio e força nos momentos difíceis de maneira direta e indireta. Agradeço também pela força para executar minhas atividades acadêmicas. Obrigado por todo incentivo e amor prestados a mim.

Quero agradecer ao meu orientador, Aldri Luiz dos Santos, pelo tempo dedicado a mim e pelas orientações que me deram suporte no decorrer do mestrado. Muito obrigado também pela confiança, paciência, compreensão e por todos os conselhos que me ajudaram a pensar não só nos assuntos do mestrado, mas também abstrair coisas do cotidiano. Agradeço também a Michele Nogueira de Lima pelos esclarecimentos e ensinamentos dedicados ao meu aprimoramento.

Aos colegas de laboratório deixo aqui meu muito obrigado pela parceria, troca de conhecimentos, amizade, descontração e pela força. Ao Alisson, ao Chicó (Danilo), ao Christian, ao Robson, a Andressa, ao Mateus, ao Danilo, ao Gustavo, ao Metuzalem, ao Benevid, ao Jefferson, ao Otto, ao Ricardo e ao Rafael. Agradeço também a amizade e a troca de conhecimentos de outros alunos. Agradeço ao Renan, ao Luiz, ao Santiago, ao Renato, ao Daniel e ao Ivan. Não posso deixar de agradecer a CAPES pela bolsa que possibilitou o meu estudo com dedicação integral e ao PPGinf.

Agradeço a todos que me influenciaram positivamente durante a caminhada do mestrado. Obrigado pela paciência e compreensão nos momentos de stress. Pelos momentos de desabafo, reclamação e cansaço nos momentos de dificuldade. Pelas palavras de sabedoria e conselhos de como lidar com as situações na vida. Deixo meu humilde muito obrigado a todos. Sem o apoio de vocês, eu não chegaria até aqui.

Resumo

O desenvolvimento das redes heterogêneas sem fio (RHSFs) apresentou uma maior abrangência de comunicação suportando a demanda dos usuários de dispositivos móveis. Isso ocorre devido à possibilidade de interoperabilidade dos dispositivos com as redes locais sem fio e redes metropolitanas. Essa interoperabilidade consiste de vários serviços de rede e permite a manutenção de conectividade durante a mobilidade do usuário. Um desses serviços consiste da autenticação do usuário que fornece o controle de acesso às redes pelo usuário. A autenticação nas RHSFs precisa lidar com a limitação de recursos dos dispositivos móveis, a transparência dos serviços dos usuários na transição de redes, e as vulnerabilidades do meio sem fio. Assim, durante o procedimento de autenticação, vários tipos de ataques podem acontecer a fim de prejudicar a confidencialidade dos usuários que portam os dispositivos móveis. Dentre os principais ataques neste serviço, destaca-se o ataque de repetição de identidade, que busca obter o acesso não autorizado aos recursos da rede. As abordagens existentes para proteger o serviço de autenticação dos ataques de repetição de identidades não levam em conta as características heterogêneas dos dispositivos, logo, elas são custosas e inseguras contra esse ataque considerando as vulnerabilidades presentes nas RHSFs. Esta dissertação propõe um esquema de autenticação chamado de ARARAS (**A**utenticação **R**esistente a **A**taques de **R**epetição de Identid**A**des em Rede**S** Heterogêneas), que tem como objetivo de anular os ataques de repetição de identidade no processo de autenticação. Esse esquema utiliza uma autenticação unificada entre as redes heterogêneas sem fio e faz uso de um mecanismo de proteção contra o ataque de repetição de identidades. Uma avaliação do esquema, a partir de simulações, analisou o desempenho e a segurança diante do ataque de repetição de identidades, comparando-o com o esquema de autenticação UHA (*Unified Handover Authentication*). Os resultados mostraram que o ARARAS detectou o ataque de repetição de identidades de forma mais eficaz e eficiente independente do tipo de tecnologia da rede e quantidade de usuários maliciosos.

Palavras-chave: redes heterogêneas, interoperabilidade, autenticação, ataque de repetição de identidade.

Abstract

The development of heterogeneous wireless networks (RHSFs) has offered a broader range of communication supporting the demand of mobile users. This is due to the possibility of interoperability of the devices with wireless local area networks and metropolitan networks. That interoperability consists of multiple network services and also allows the maintenance of connectivity during the mobility of the user. One of those services consists of the user authentication, which enables user access control to networks. Hoever, authentication in RHSFs needs to deal with the limitation of mobile device resources, the transparency of user services in network transition, and also wireless vulnerabilities. In this way, over the authentication procedure, various types of attacks may occur in order to impair the confidentiality of users who carry mobile devices. Among the main attacks on this service, we highlight the attack of repetition of identity, which seeks to obtain unauthorized access to network resources. On other the hand, the current approaches to protect the authentication service from identity replay attacks do not take into account the heterogeneous features of the devices, so they become costly and insecure against this sort of attack considering the vulnerabilities present in RHSFs. This dissertation proposes an authentication scheme called ARARAS (**A**utenticação **R**esistente a **A**taques de **R**epetição de Identid**A**des em Rede**S** Heterogêneas), which aims avoiding attacks of identity replay under the authentication process. Thus, the scheme uses unified authentication between heterogeneous wireless networks, as well as makes use of a mechanism to defense it against identity replay. An evaluation of ARARAS by simulations analyzed its performance and security in face of identity replay attacks, also compared it to the Unified Handover Authentication (UHA) authentication scheme. The results pointed out that ARARAS is more effective to detect detected identity replay attacks regardless of the type of network technology and the number of malicious users.

Keywords: heterogeneous networks, interoperability, authentication, identity replay attack.

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Acrônimos

RHSF	Redes heterogêneas sem fio
AG	Autenticador global
AL	Autenticador local
AP	Ponto de acesso
UE	dispositivo do usuário
ePDG	Evolved Packet Data Gateway
EPC	Evolved Packet Core
LTE	Long-Term Evolution
ARARAS	Autenticação resistente a ataques de repetição de identidades em redes
RI	Ataque de repetição de identidades
UHA	Unified handover autthentication
WAPI	Wireless Authentication and Privacy Infrastructure
LRA	Lightweight roaming authentication
GBHA	Group-based Handover Authentication
PH	PairHand
HH	HashHand
LAP	Lightweight authentication protocol
PPS	Pre-authtentication protocol with symmetric keys
HACH	Handover authentication using credentials and chameleon hash
FHA	Fast handover authentication
PBA	Prediction-based authentication
IACPK	Identity-based Access Authentication Scheme
LRA	Lightweight Roaming Autentication
GHAP	Group handover authentication protocol

Lista de Símbolos

T_{exp}	Tempo de expiração da autenticação
T_{rec}	Tempo de recebimento de autenticação
H	Conjunto de redes heterogêneas
AP	Conjunto de pontos de acesso
ap	Ponto de acesso
qt	Quantidade de mensagens recebidas
C_w	Conexão de um nó
I	Conjunto de identidades
IR	Conjunto de identidades relacionadas
N	Dispositivo móvel
G	Grupo cíclico aditivo
GT	Grupo cíclico multiplicativo
P	Gerador de G
Aut	Autenticadores
M	Mensagem
A	Assinatura
Aut	Autenticadores
T_{prev}	Taxa de ataques de repetição identidade prevenidos
T_{fa}	Taxa de falso positivos
T_x	Tempo médio de transmissão entre dispositivo móvel e ponto de acesso
T_y	Tempo médio de transmissão entre pontos de acesso
T_z	Tempo médio de transmissão entre ponto de acesso e autenticador
C_{ini}	Custo computacional da inicialização
C_{aut}	Custo computacional da autenticação
C_{aut}	Custo computacional da autenticação

Capítulo 1

Introdução

O desenvolvimento dos meios de comunicação sem fio e o avanço da tecnologia dos dispositivos móveis juntamente com a grande demanda de usuários conduziram uma nova padronização para implantação das redes de comunicação [1]. Esse novo padrão permite às redes de comunicação que possuem tecnologias diferentes (LTE, 802.11, WiMAX, etc.) ofereçam a manutenção da conectividade para os dispositivos computacionais. Para isso, o ambiente de redes de comunicação sem fio deve possuir diversos pontos de acesso para atender a demanda por conectividade dos dispositivos móveis. Ademais, esses dispositivos móveis dos usuários precisam interagir com os pontos de acesso das redes heterogêneas sem fio para fornecer serviços.

As redes heterogêneas sem fio (RHSFs) compõem uma infraestrutura composta por vários tipos de redes que usam tecnologias de acesso sem fio diferentes e independentes [2, 3]. Essas redes interoperam para prover cobertura de acesso e a transferência de conexão aos dispositivos móveis. Desta forma, as RHSFs conseguem manter a disponibilidade dos serviços ao usuário final. A proliferação rápida e generalizada desses dispositivos móveis que integram diferentes formas de comunicação resultou no aumento intensivo de dados que tem crescido a um ritmo sem precedentes nos últimos anos [4]. A infraestrutura, em geral, opera através da interoperabilidade das redes sem fio metropolitanas, que possuem cobertura em uma região ampla, e locais para prover conexão durante a mobilidade do usuário [5].

A interoperabilidade entre as redes heterogêneas tem a função de suportar as necessidades dos usuários de modo a diminuir os problemas das infraestruturas das redes e oferecer um ambiente de computação ubíquo. Alguns dos serviços voltados aos usuários finais abrangem diversas áreas como saúde, militar, transporte, entretenimento e telecomunicações como apresenta a Figura 1.1. No entanto, a conexão está sujeita a atrasos de pacotes e com isso prejuízos nos serviços utilizados pelos usuários. Isso se torna mais frequente quando existe a necessidade do usuário se mover de um local para outro. A mobilidade do usuário em um cenário heterogêneo de redes requisita do dispositivo móvel a transição de conectividade entre as redes sem fio.

A mobilidade do usuário em um cenário heterogêneo de redes requisita do dispositivo móvel a transição de conectividade entre as redes sem fio. Esta transição ocorre entre um dispositivo móvel e dois pontos de acesso de rede que representam o ponto de acesso origem e ponto de acesso destino. Desta forma, na gerência de mobilidade se torna essencial o serviço de transição de redes (*Handover*) para transferir a conexão do dispositivo móvel de maneira mais transparente possível ao usuário [3]. A necessidade desse serviço ocorre por diversos motivos no ambiente de redes sem fio, como por exemplo a qualidade da conexão para atender a demanda de algum usuário. No serviço de transição, o usuário móvel deve realizar o processo de autenticação para se conectar a nova rede.

Figura 1.1: Redes heterogêneas e os serviços

A autenticação consiste de um serviço fundamental para o uso da computação moderna pois permite que sistemas computacionais reconheçam os usuários e seus dispositivos [6]. O reconhecimento ou identificação de um dispositivo em redes de computadores proporciona ao usuário o uso de recursos e serviços de forma a garantir a confidencialidade e disponibilidade. A autenticação do usuário através do dispositivo móvel ocorre de diversas formas entre as redes heterogêneas devido aos diferentes padrões de comunicação e necessidades de cada tipo de rede. Assim, a autenticação deve adaptar-se as diferenças durante o serviço de transição de redes sendo necessário um esquema ou controle de autenticação. O controle de autenticação gerencia a maneira como a autenticação ocorre. Apesar do controle de autenticação ser um serviço para o acesso dos usuários à rede de maneira segura, existem várias questões a serem exploradas.

As principais questões em relação ao controle de autenticação em redes heterogêneas são o desempenho e a segurança durante a transição [7]. O desempenho da autenticação leva em consideração o custo computacional e o tempo para a autenticação ser efetuada. Devido à heterogeneidade das redes, o custo computacional e o tempo de autenticação podem variar e assim dificultar a transparência do serviço de transição de rede, resultando em prejuízos na experiência do usuário durante a mobilidade. Em relação à segurança, os problemas de autenticação na integração das redes se baseiam no relacionamento entre as entidades que constituem cada rede [8]. Deste modo, a manutenção da confidencialidade e disponibilidade do serviço de autenticação tem se tornado um desafio devido à conexão com a rede no momento da mobilidade do usuário acontecer no meio sem fio, sendo vulnerável a ataques. Por ser uma transmissão de dados sem fio, ela está sujeita a ataques que tem como objetivo a escuta do tráfego de dados, captura de dados e negação do serviço de autenticação. Outro desafio de segurança em relação a heterogeneidade deriva das vulnerabilidades específicas de cada rede em virtude das características de comunicação [9]. Fornecer uma autenticação durante a transição de redes de forma transparente e segura tem sido um desafio importante.

1.1 Motivação

Os ataques mais frequentes contra a autenticação durante o processo de transição têm como principal característica a captura de dados da autenticação do dispositivo móvel e do ponto

de acesso. Esses ataques nas entidades das redes ocorrem com a captura dos quadros no decorrer da comunicação, onde, o atacante pode efetuar a personificação de identidade de um dispositivo ou tornar indisponível o serviço de autenticação, impedindo a transição de conexão para outra rede. Dentre os ataques de quadros mais frequentes, o ataque de repetição de identidade (RI) tem se destacado em comunicações de redes WWAN e WLAN devido a ausência de métodos que tratem os quadros na interconexão das redes [10, 11]. O atacante efetua a captura dos quadros da mensagem de autenticação e replica esses quadros para os dispositivos da rede. Assim, o dispositivo móvel ou ponto de acesso armazena em sua tabela de roteamento rotas de comunicação erradas [12]. Assim, as mensagens de autenticação são enviadas para o dispositivo do atacante. O RI pode ser utilizado para personificar as entidades da rede ou simplesmente para perturbar o funcionamento do roteamento [13]. Através da personificação, o atacante pode se passar por um outro dispositivo da rede para obter acesso ou informações, afetando a confidencialidade. O ataque RI se executado de modo contínuo tem, a capacidade de esgotar os recursos de hardware dos dispositivos.

Algumas estratégias de autenticação utilizam funções de emparelhamento [14, 7] com o objetivo de obter um menor custo computacional e tempo. Devido a busca por um melhor desempenho, essas estratégias possuem vulnerabilidades pois desconsideram que a captura e replicação dos quadros de autenticação pode ser utilizada em outra rede. As estratégias de segurança propostas possuem foco nos ataques de negação de serviço e *sniffing* [15, 16, 17]. No entanto, esses trabalhos não são eficazes em impedir que um atacante que utiliza o ataque RI tenha acesso a rede pois desconsideram a possibilidade desses quadros serem usados para obter acesso em outros pontos de acesso da rede e não existir um tratamento de quadros que identifique a unicidade. Na autenticação, o problema consiste em aliar desempenho e segurança na mobilidade do usuário. Além disso, a necessidade de transição entre as redes ocasiona a possibilidade dos quadros de mensagens de autenticação serem usados por um atacante. Para que a autenticação atenda as necessidades do serviço de transição entre redes é necessário um controle de autenticação leve em questão de custo computacional, rápido em relação ao tempo de autenticação e seguro para fornecer ao usuário a confidencialidade e a disponibilidade.

Os métodos utilizados para prevenir o ataque RI tem como base o tempo de autenticação que acontece no instante de requisição de conexão entre o dispositivo móvel e o ponto de acesso [18]. Apesar do tempo de autenticação auxiliar a prevenção desse ataque para uma rede, esse método não funciona quando o ataque ocorre em redes heterogêneas [19]. Devido à diversidade de redes, o atacante pode usar esses quadros contra diversas entidades de redes durante um intervalo de tempo. Assim, a integração entre as redes de telecomunicações e redes locais sem fio possui vulnerabilidades pois um usuário malicioso que executa esse ataque pode corromper a comunicação de diversos dispositivos e redes de tecnologias diferentes.

1.2 Objetivos

Este trabalho tem como objetivo tornar o serviço de autenticação em redes heterogêneas resistente a ataques de repetição de identidades nas redes heterogêneas diante da execução da autenticação no serviço de transição vertical. Para alcançar esse objetivo, propõe-se um esquema para auxiliar o serviço de autenticação a redes heterogêneas de garantir as propriedades de confidencialidade e de disponibilidade no processo de handover e assim detectar identidades repetidas por um atacante na infraestrutura de redes.

O controle do serviço de autenticação deve suportar as mensagens de autenticação entre as entidades da rede, e garantir que os quadros dessas mensagens sejam válidos no processo de autenticação. O controle de autenticação proposto simplifica o modo como a autenticação

acontece e rejeita mensagens derivadas de ataques de repetição de identidades. Para isso, o controle de autenticação realiza a autenticação unificada entre a redes e compõe duas fases de autenticação com um mecanismo para verificação de quadro de mensagem. Essas fases juntamente com o mecanismo impedem que o ataque de repetição tenha êxito.

A unificação da autenticação descreve um controle de autenticação que padroniza o modo como a autenticação acontece para redes de diferentes tecnologias [20]. Com a autenticação unificada a mesma regra de autenticação para obter conexão se torna possível para redes de diferentes tecnologias. Com o auxílio de um autenticador central de rede, a gerência de chaves e identidades dos usuários que se conectam na rede se torna mais rápida e oferece uma gerência mais robusta para detecção de atacantes e intrusos na rede heterogênea. Essa estratégia permite a interconexão de redes do tipo WWAN com a rede WLAN.

O dispositivo móvel através do controle de autenticação deve efetuar a requisição de conexão primeiramente na rede WWAN. Essa estratégia permite ao usuário obter as chaves de acesso de uma fonte segura. Com essas chaves o dispositivo pode se autenticar em outros pontos de acesso WWAN e da rede WLAN no momento de transição. Assim, o esquema de autenticação proposto possui a gerência das identidades e chaves utilizando uma autenticação unificada, funções para garantir que a mensagem não seja facilmente compreendida pelo atacante e um mecanismo de verificação do quadro da mensagem de autenticação recebida pela rede.

1.3 Contribuições

Este trabalho apresenta as seguintes contribuições:

- Um estudo sobre os esquemas de autenticação que visam a proteção contra os ataques de repetição de identidade existentes na literatura. Esses esquemas foram classificados de acordo com as características das redes e em criptografia. Através desse estudo foi possível levantar os requisitos necessários para a detecção desse ataque no serviço de autenticação.

- Uma quantificação do desempenho e da segurança por meio de simulação de um dos trabalhos encontrados na literatura em um ambiente de redes heterogêneas sem fio. Para realizar essa quantificação, o critério adotado foi o esquema que mais se adapta ao problema tratado e também mais compatível com o ambiente heterogêneo. Dessa maneira, o esquema UHA foi escolhido uma vez que ele é o mais adequado para o ambiente de redes heterogêneas.

- Uma especificação do esquema de autenticação ARARAS para o serviço de transição nas redes heterogêneas sem fio. O ARARAS possui duas fases, a inicialização e a autenticação. Essas duas fases juntas possibilitam a integração entre redes de tecnologias diferentes e uma gerência simplificada das identidades e chaves dos dispositivos móveis. O esquema proposto conta ainda com um mecanismo de proteção para inviabilizar o ataque de repetição de identidade na transição vertical nas redes heterogêneas.

- Uma avaliação do esquema ARARAS diante de ataques de repetição de identidade. A avaliação considerou um cenário composto por um ambiente de redes heterogêneas. Ademais, o ARARAS foi comparado com o esquema UHA possui como base as métricas de segurança e desempenho, onde em ambos o ARARAS obteve melhores resultados. A avaliação mostrou que o esquema ARARAS inviabiliza os ataques RI independente do tipo de tecnologia de rede.

1.4 Estrutura da dissertação

Esta dissertação está organizada em seis capítulos. O Capítulo 2 apresenta os fundamentos relacionados às redes heterogêneas sem fio (RHSF), à transição em redes heterogêneas sem fio, ao serviço de autenticação e ao ataque de repetição de identidade, os quais mostram os desafios para prover uma autenticação segura para os dispositivos móveis. Em seguida, o Capítulo 3 classifica e caracteriza as técnicas de autenticação utilizadas para o controle de acesso dos dispositivos móveis nas redes. Já o Capítulo 4, descreve o esquema de autenticação para as redes heterogêneas sem fio (ARARAS) que identifica ataques de repetição de identidade. O Capítulo 5 apresenta as avaliações de desempenho e de segurança composta por um cenário realístico e a mensuração dos esquemas de autenticação ARARAS e UHA. Por fim, o Capítulo 6 conclui este trabalho apresentando também as suas direções futuras.

Capítulo 2

Fundamentos

Este capitulo apresenta os fundamentos necessários para o entendimento do contexto do problema tratado na dissertação e da solução apresentada. A Seção 2.1 introduz as características gerais de comunicação e autenticação das redes heterogêneas sem fio. A Seção 2.2 aborda em detalhes o processo de transição em redes heterogêneas. A Seção 2.3 descreve o processo de autenticação e o ataque de repetição de identidades.

2.1 Redes heterogêneas sem fio

A expansão das redes de telecomunicações e o aumento do uso de aparelhos celulares ocasionou a necessidade de interconexão entre as diversas tecnologias de redes para expandir a comunicação, surgindo as redes heterogêneas (HetNet) [21]. As redes heterogêneas consistem de diversos tipos de redes que utilizam diferentes e independentes tecnologias de acesso sem fio [22]. Essas redes compreendem diversas tecnologias como a telefonia celular, as redes de transmissão de TV e a Internet oferecendo serviços específicos. Cada tecnologia de rede possui sua própria característica de segurança, qualidade de serviço, largura de banda, frequência, área de cobertura e custo. A RHSF proporciona ao usuário uma melhor cobertura de comunicação e conexão para utilizar serviços de diversas áreas como multimídia, serviços relacionados a áreas da saúde, militar e financeiro. Para uso desses serviços na RHSF, existe a necessidade de comunicação entre alguns dispositivos de rede.

Os principais componentes das redes sem fio heterogêneas são o Dispositivo Móvel, Ponto de Acesso e o Núcleo Central da Rede [23]. A Figura 2.1 ilustra um ambiente de redes heterogêneas onde o usuário se movimenta obtendo conectividade. Os dispositivos móveis utilizados pelos usuários da rede possuem diferentes características de hardware e assim diferentes configurações de mobilidade e interfaces de comunicação sem fio que suportam o acesso às tecnologias da RHSF. O ponto de acesso de uma rede proporciona ao dispositivo móvel a conectividade para que os recursos e serviços sejam adquiridos pelos usuários. O núcleo central da rede gerencia o acesso para conexões e os recursos disponibilizados para um dispositivo móvel. Esse núcleo compreende diversos serviços de rede que oferecem segurança de controle de acesso.Além disso, o núcleo central da rede se comunica com o dispositivo móvel através do ponto de acesso nas tecnologias RHSF.

As redes heterogêneas se comunicam através da interoperabilidade. A Interoperabilidade consiste na capacidade que um sistema tem de se comunicar de modo transparente com outro sistema [24]. Essa interoperabilidade no contexto de redes de computadores representa a capacidade que as redes, de tecnologias homogêneas ou heterogêneas, possuem para interagirem mantendo a comunicação e fornecimento de serviços para um dispositivo durante a

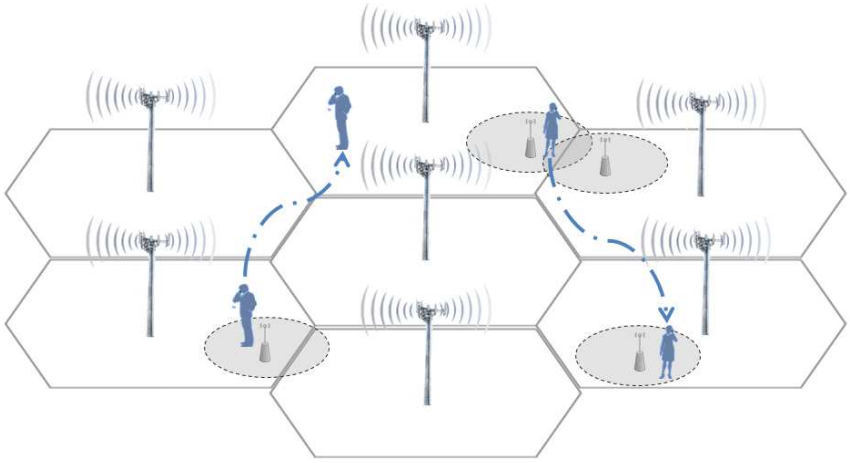


Figura 2.1: Mobilidade do usuário

mobilidade [**?**]. Para atender a interação e assim prover a comunicação para o dispositivo móvel são estabelecidos padrões, regras ou procedimentos. Os padrões determinam a forma como a interoperabilidade das redes se sucede [25]. Isso permite a extensão das operações e funcionalidades de serviços para o usuário e também a otimização de recursos através de um gerenciamento da conexão de um dispositivo móvel.

O gerenciamento da conexão nas redes heterogêneas representa um componente do gerenciamento de mobilidade que garante a continuidade da conectividade de um dispositivo móvel de um ponto de acesso origem para o ponto de acesso destino [26]. Isso é feito transferindo a ligação do nó móvel entre os diferentes pontos de acesso disponíveis no meio quando necessário. Esse procedimento é conhecido como serviço de transição. O serviço de transição deve efetuar a transição entre redes de modo que não ocorra perda de qualidade no serviço utilizado pelo usuário do dispositivo móvel.

O gerenciamento da conexão nas redes heterogêneas representa um componente do gerenciamento de mobilidade que garante a continuidade da conectividade de um dispositivo móvel de um ponto de acesso origem para o ponto de acesso destino [26]. Isto é feito transferindo a ligação do nó móvel entre os diferentes pontos de acesso disponíveis no meio quando necessário. Este procedimento é conhecido como serviço de transição. O serviço de transição deve efetuar a transição entre redes de modo que não ocorra perda de qualidade no serviço utilizado pelo usuário do dispositivo móvel.

2.2 Transição em redes heterogêneas

A mobilidade do usuário atua sobre a comunicação e continuidade da conexão entre um dispositivo móvel e uma rede, sendo necessário o serviço de transição. A transição trata do processo de terminar uma conexão de rede existente em um ponto de acesso para iniciar uma nova conexão com um ponto de acesso destino [27]. Esse serviço de transição (*Handover*) permite a continuidade de serviços utilizados pelo usuário na mudança de conexão entre as redes. O processo de transição permite que o dispositivo móvel se conecte entre as redes de tecnologias diferentes [28]. Em redes heterogêneas a conectividade se torna fundamental para o usuário que precisa obter serviço mesmo transitando por redes com características e requisitos de conectividade diferentes.

O processo de transição ocorre quando o dispositivo móvel necessita da continuidade da comunicação sem fio durante a mobilidade [29]. A mobilidade do usuário acarreta na variação da

qualidade de sinal na conexão com a estação base que afeta os serviços. Para que esses serviços não sejam afetados, o dispositivo móvel reconhece as possíveis redes para conexão e executa a transição de conexão. A transição de conexão pode ocorrer de duas formas que são o *handover* horizontal e *handover* vertical.

O processo de *handover* horizontal ocorre entre tecnologias de acesso idênticas que estão em células diferentes durante a mobilidade do usuário [28]. Devido ao *handover* horizontal acontecer em tecnologias idênticas, em geral, o handover horizontal é mais simples, mas não é livre de problemas e também pode afetar a qualidade de experiência do usuário. O *handover* vertical acontece de maneira mais complexa devido à cada rede ter suas próprias características de frequência, autenticação, alcance e qualidade de serviço. Essa diferença se torna um problema pois o *handover* vertical deve acontecer de maneira transparente sem prejudicar a qualidade de experiência do usuário e também ser segura, preservando a confidencialidade e disponibilidade dos serviços e recursos da rede.

O *handover* vertical possui três fases: coleta de informação, decisão e execução. A fase da coleta de informação no *handover* vertical obtêm informações de preferências de usuário de rede [30]. O usuário pode ter preferências por redes que possuem segurança, desempenho ou regras de conexão. A fase de decisão do *handover* vertical escolhe a melhor rede disponível no raio de alcance do usuário para se conectar com base nas informações colhidas na fase anterior. A fase de execução faz com que o dispositivo se conecte com a rede escolhida. Para efetuar o *handover*, o dispositivo deve se autenticar na rede escolhida para obter acesso.

2.3 Serviço de autenticação

O processo de autenticação é aquele capaz de determinar se alguém é quem está dizendo ser [31]. O compartilhamento de recursos e serviços em diversos contextos traz a necessidade de uma organização de gerência de acesso suportada pela autenticação. Essa gerência de acesso tem como benefícios a autenticidade de informação e garantia de legitimidade de usuários para usar recursos e serviços. Isso permite que as pessoas possam exercer suas tarefas de forma mais organizada e segura.

O processo de autenticação possui diversas abordagens para serem aplicadas em diversos contextos. Essas abordagens durante o processo de autenticação são classificadas em o que você é, o que você tem e o que você sabe [32]. A abordagem com base no que você é tem como objetivo identificar usuários através de características físicas utilizando a biometria. A autenticação como base no que você tem requisita do usuário credenciais para comprovar que o usuário pode utilizar o serviço. A abordagem com base no que você sabe requisita do usuário uma senha ou segredo de conhecimento do usuário.

Em redes de computadores a autenticação tem o objetivo de fornecer ao usuário de dispositivo computacional o acesso à conexão com uma rede através de um ponto de acesso para utilização de recursos e serviços [33]. A autenticação no contexto de redes efetua troca de mensagens para confirmação de identidade do usuário entre o dispositivo móvel e ponto de acesso. Essas mensagens utilizadas representam a forma como foi padronizado o esquema de autenticação. Assim, esse esquema estabelece uma organização para envio de requisição de conexão e resposta de autenticação. Para assegurar essa comunicação entre as entidades dispositivo computacional e ponto de acesso necessita da utilização de esquemas de chaves.

Os esquemas de chaves utilizados por um esquema de autenticação são a chave simétrica (secreta) e assimétrica (pública e privada) [33]. A chave simétrica representa uma senha usada tanto pelo remetente para codificar a mensagem numa ponta, como pelo destinatário para

decodificá-la na outra [34]. A principal vantagem é a simplicidade, essa técnica apresenta facilidade de uso e rapidez para executar os processos criptográficos. A desvantagem é não garantir a autenticidade e não-repúdio. Na chave assimétrica cada parte envolvida na comunicação usa duas chaves diferentes (assimétricas) e complementares, uma privada e outra pública [35]. Nesse caso, as chaves não são apenas senhas, mas arquivos digitais mais complexos (que eventualmente até estão associados a uma senha). A chave pública pode ficar disponível para qualquer pessoa que queira se comunicar com outra de modo seguro, mas a chave privada deverá ficar em poder apenas de cada titular.

A grande vantagem desse sistema é permitir a qualquer um enviar uma mensagem secreta, apenas utilizando a chave pública de quem irá recebê-la. Como a chave pública está amplamente disponível, não há necessidade do envio de chaves como feito no modelo simétrico. A confidencialidade da mensagem é garantida, enquanto a chave privada estiver segura. Caso contrário, quem possuir acesso à chave privada terá acesso às mensagens. O óbice desse sistema é a complexidade empregada no desenvolvimento dos algoritmos que devem ser capazes de reconhecer a dupla de chaves existentes e poder relacionar as mesmas no momento oportuno, o que ocasiona um grande poder de processamento computacional.

Os principais problemas relacionados à autenticação em redes heterogêneas são a interoperabilidade, custo computacional, tempo de autenticação, confidencialidade, disponibilidade e resistência a ataques [7]. A resolução desses problemas auxília o usuário portador do dispositivo móvel à conectar-se nas redes heterogêneas, como mostra a Figura 2.2. Os ataques mais frequentes de autenticação em redes heterogêneas são os ataques que utilizam de quadros (*frames*) de controle. Com os quadros de controle, o atacante da rede pode capturar informações e com isso replicar ou modificar estes quadros para obter acesso ou negar serviço de autenticação. Dentre os ataques de *frames* que ocorrem em redes heterogêneas, o mais comum é o ataque de repetição de identidades.

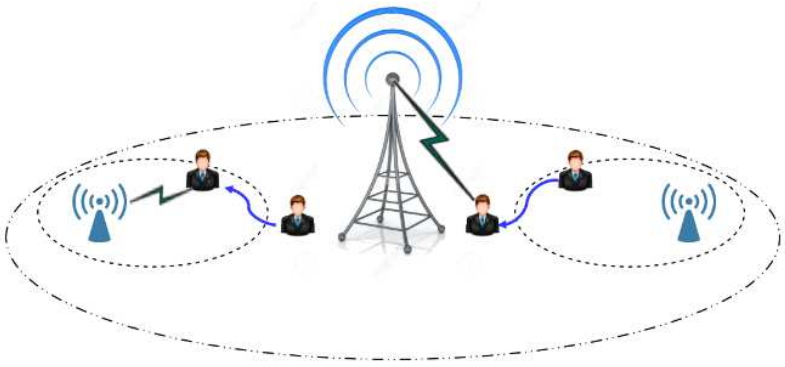


Figura 2.2: Requisitos de segurança

2.4 Ataque de repetição de identidades

O ataque de repetição de identidades (RI) consiste na captura da informação das mensagens entre duas entidades de rede e na sua replicação para obter privilégios ou confundir serviços [8]. Através do ataque RI, um usuário malicioso pode se beneficiar dos direitos de acesso aos recursos e serviços de um usuário comum [36]. No serviço de autenticação, o usuário normalmente envia sua identidade e senha criptografada para um servidor com a finalidade de

efetuar o acesso a rede. Contudo, se o atacante intercepta a comunicação, esse pode repetir a sequência de quadros de autenticação para obter os mesmos direitos que o usuário; bem como proporcionar a troca de senhas e afetar a confidencialidade do usuário. Esse ataque pode ser realizado por um usuário malicioso de diversas maneiras, podendo afetar também a disponibilidade do serviço de autenticação e esgotar recursos tanto da rede como do usuário móvel.

Os tipos de ataque de repetição de identidade fundamentam-se na captura das informações durante a transmissão das mensagens de autenticação [37]. A Figura 2.3 apresenta um dos métodos de ataque. Assim como outros ataques de quadro, esse ataque efetua a captura dos quadros pelo meio sem fio entre um dispositivo móvel (UE) e um ponto de acesso (AP) durante o processo de autenticação com o servidor de uma rede. Através da obtenção desses quadros, o atacante pode replicá-los para um ponto de acesso e obter acesso à rede, recursos e serviços autorizados do usuário proprietário dos quadros de autenticação.

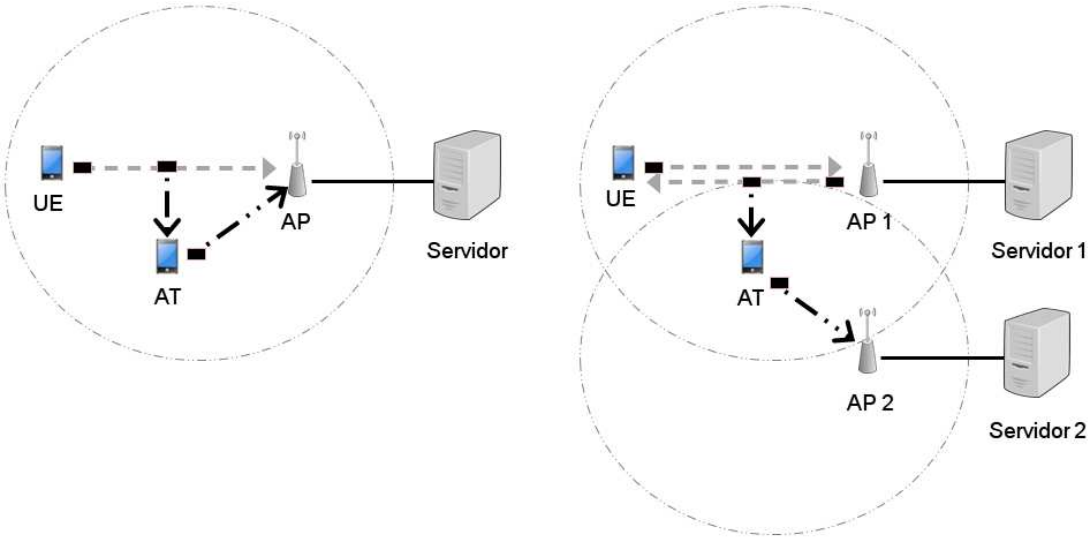


Figura 2.3: Ataque de repetição de identidades para a rede

O ataque RI também compreende outra forma de ataque. A Figura 2.4 mostra o funcionamento desse ataque. A captura de quadros de resposta do ponto de acesso durante o envio de mensagens para o dispositivo móvel replicá-los para o dispositivo móvel com a finalidade de obter informações de autenticação da vítima ou servir como um ponto de acesso falso. O atacante pode também efetuar um ataque de negação de serviço na rede com os quadros de identidade da vítima. A negação de serviço pode ser também executada replicando a mensagem de resposta da rede no dispositivo móvel, esgotando os recursos.

Uma entidade de gerência de identidade para as redes tem sido implementada para auxiliar a integração de diferentes tecnologias. Essa estratégia apresenta um método que auxilia o dispositivo a se autenticar entre as redes de forma mais rápida. No entanto, essa gerência possui vulnerabilidades de personificação de identidades. Desta forma, o ataque RI pode ser mais danoso em questões de confidencialidade e disponibilidade [38]. Devido à variedade de tecnologias de rede e a integração entre elas, o atacante possui mais oportunidades para realizar a captura de quadros e replicar as informações da mensagem de autenticação do usuário entre as redes a fim de obter acesso não autorizado. Assim, um controle de autenticação deve auxiliar na forma como as identidades são distribuídas e a autenticação deve ser realizada [39].

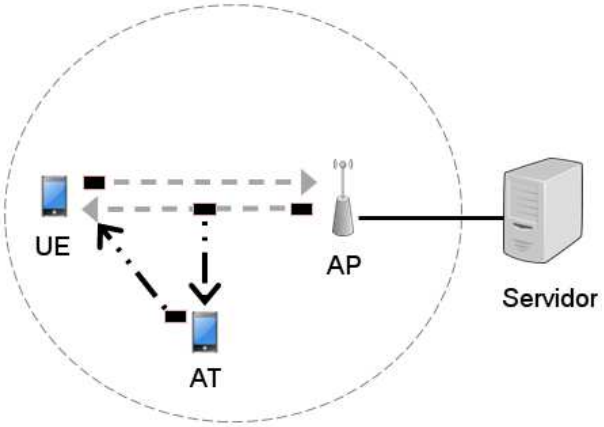


Figura 2.4: Ataque repetição de identidades para o dispositivo móvel

2.5 Resumo

Este capítulo apresentou os fundamentos acerca das redes heterogêneas, mostrando as suas características de funcionamento. Além disso, foram descritos os requisitos de transição de redes e o serviço de autenticação juntamente com os requisitos necessários a serem atendidos nas redes heterogêneas. Os requisitos abrangem os aspectos de segurança e desempenho no serviço de autenticação. Os aspectos de segurança compreendem a confidencialidade e a disponibilidade. Os aspectos de desempenho consistem do tempo de execução e custo de processamento do serviço de autenticação. Finalmente, o ataque RI foi apresentado através de figuras.

Capítulo 3

Técnicas de Autenticação

Este capítulo apresenta os principais trabalhos existentes na literatura que propõe métodos de autenticação que lidam com redes heterogêneas. A Seção 3.1 apresenta as propriedades das técnicas de autenticação baseadas na identidade. A Seção 3.2 expõem as características das técnicas de autenticação baseadas em grupo. A Seção 3.3 mostra as propriedades das técnicas baseadas em pareamento.

3.1 Classificação das técnicas de autenticação

Esta seção apresenta a classificação das técnicas de autenticação presentes na literatura e investigada na dissertação. As técnicas de autenticação classificadas na forma de diagrama descrita na Figura 3.1. As abordagens estão organizadas em relação a identidade, baseada em grupo de chaves e emparelhamento bilinear. Outras estratégias são apresentadas nesse capítulo com a finalidade de analisar as técnicas apresentadas em outros contextos de redes e desafios.

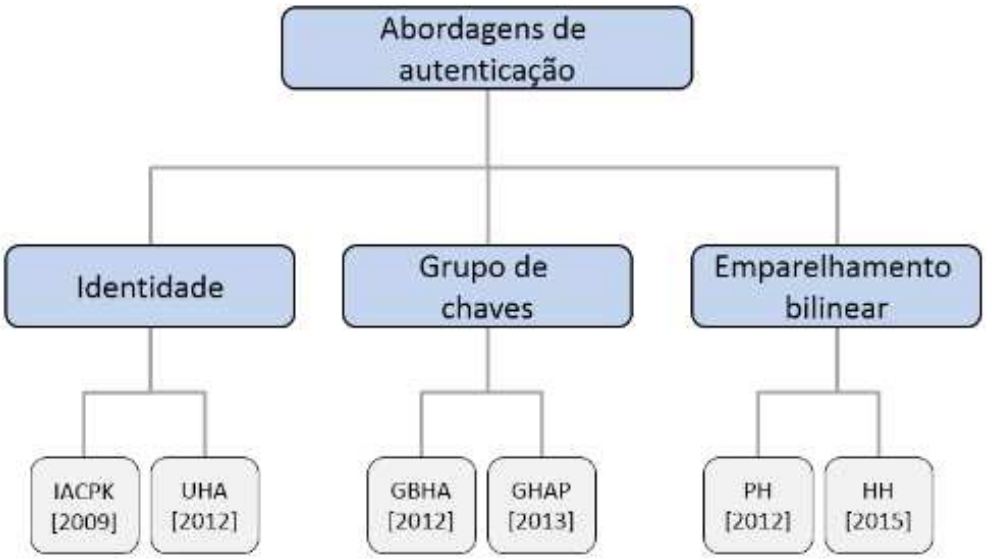


Figura 3.1: Classificação das técnicas

3.2 Autenticação baseada em identidade

O controle de autenticação IACPK (*Identity-based Access Authentication Scheme*) [16] baseia-se na tecnologia CPK para realizar uma autenticação de identidade temporária com o propósito de proteger a privacidade do usuário e oferecer anonimato. A tecnologia CPK se trata de um tipo de algoritmo de criptografia baseado em identidade que utiliza curvas elípticas que compõem um modelo de gerência de chaves centralizado. Este modelo de gerência de chaves tem como suporte o algoritmo ECDH (curva elíptica do protocolo Diffie-Hellman) que oferece melhoras no protocolo de autenticação.

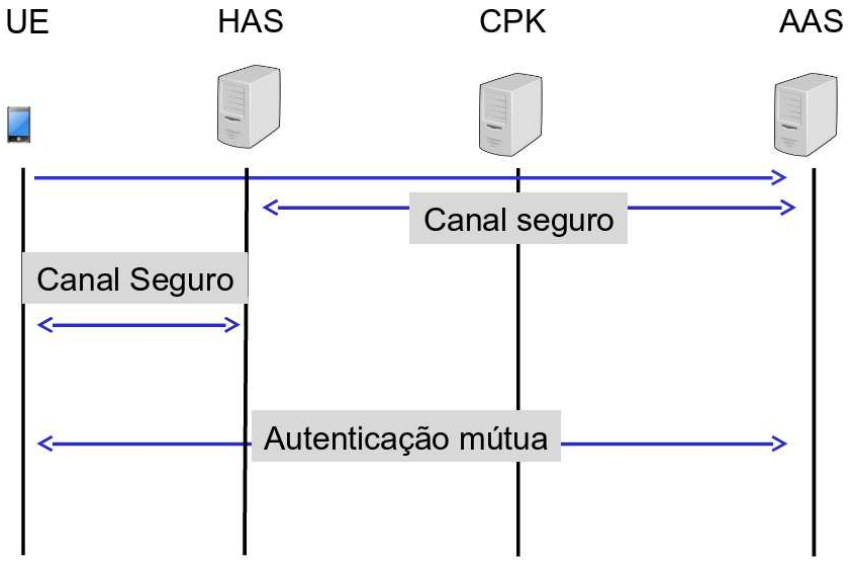


Figura 3.2: Autenticação do esquema IACPK

A Figura 3.2 mostra o funcionamento do controle de autenticação. O dispositivo móvel (UE) envia as mensagens de autenticação para o servidor de serviço de autenticação (ASS) da rede a ser visitada. Este autenticador ASS contacta o servidor de serviço doméstico (HAS) para verificar a identidade do UE. Esta estratégia permite que um UE se conecte a uma nova rede através uma identidade temporária gerada no ASS. A troca de informações entre HAS e ASS tem suporte do algoritmo Diffie-Hellman estabelecendo um canal seguro para comunicação. O canal seguro entre estas identidades auxilia no momento da distribuição das chaves públicas do ASS e UE. A geração de chaves públicas do protocolo de autenticação IACPK ocorre através da conexão com a internet onde existe um servidor central para gerência de chaves com base no CPK. Isto torna a estratégia inviável pois o custo de tempo para que a autenticação de um dispositivo aconteça se torna elevado. O IACPK apresenta mecanismos contra o ataque de repetição de identidades (RI) que são o *timestamp* e o número randômico. O *timestamp* fornece uma tolerância de tempo de mensagem e o número randômico proporciona segurança à chave privada. Estes mecanismo adotados pelo esquema IACPK não garantem que o ataque de repetição afete as redes. Neste esquema o ataque poderia ser utilizado para negar o serviço dos pontos de acessos. Outra forma de ataque seria replicar os quadros em outro ponto de acesso.

O esquema UHA (*Unified Handover Authentication*) [17] consiste de um processo de autenticação simples que utiliza como proteção de segurança PFS (*Perfect Forward Secrecy*) e MKFS (*Master Key Forward Secrecy*). Este esquema funciona através de uma requisição de autenticação inicial feita na rede LTE através de um gerenciador de chave central com o objetivo de gerenciar conexões entre redes 3GPP e não 3GPP. Assim, acontece uma autenticação mútua entre as entidades da rede que são o dispositivo móvel (UE), o gerenciador de mobilidade (MME)

e o gerenciador de chave central (KGC). O UE requisita uma identidade para o KGC pelo qual envia a chave pública S e a chave randômica R.

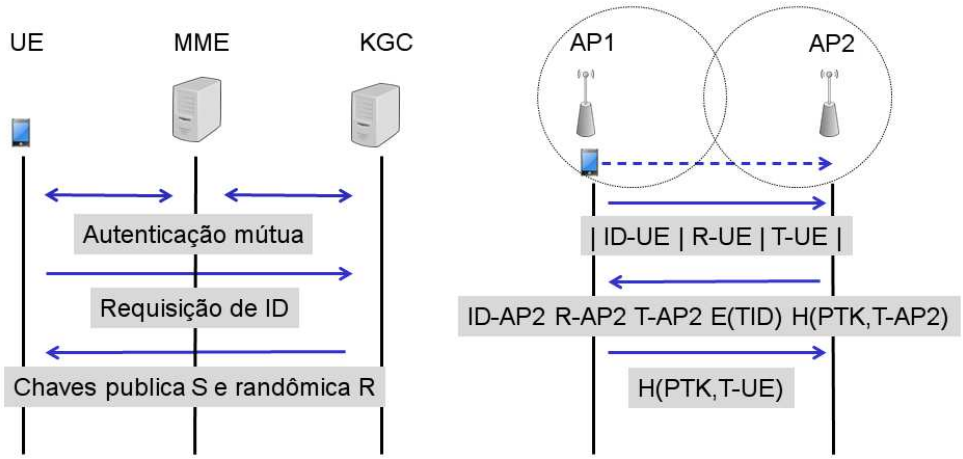


Figura 3.3: Autenticação do esquema UHA

A Figura 3.3 apresenta a autenticação na transição vertical onde trocas de identidades, chaves e tempo de envio. Primeiramente o dispositivo móvel requisita autenticação com a rede LTE para obtenção de chaves. Com estas chaves, o dispositivo móvel pode se autenticar com as demais redes. No processo de handover o UE apresenta ao ponto de acesso (AP) sua identidade e chave pública. O AP responde enviando a identidade e sua chave pública. Desta forma, o UE verifica e descriptografa a mensagem para obter uma identidade temporária aceita pelo ponto de acesso. Assim, o UE envia uma reposta contendo a chave aceita pelo AP. Apesar do esquema usar chaves assimétricas e tempo de autenticação, o UHA garante a unicidade da mensagem de requisição para o ponto de acesso. O atacante pode efetuar a escuta de todos os pacotes de transmissão entre o UE e o AP tendo a capacidade de efetuar a replicação dos quadros de autenticação para o mesmo ponto de acesso. Deste modo, o atacante consegue obter a identidade na rede LTE e em redes tecnologias diferentes. O ataque de repetição de identidades pode afetar além da confidencialidade, a disponibilidade no esquema UHA esgotando os recursos dos pontos de acesso.

Nesta abordagem de controle de autenticação, um centro de geração de chaves se torna necessário para as identidades dos dispositivos da rede. Na fase de inicialização, cada dispositivo recebe sua identidade e seus pares de chaves públicas e privadas. O centro de geração escolhe aleatoriamente uma chave privada para cada nó e publica sua chave pública correspondente. Em seguida, a fase de registro de usuário, onde cada usuário envia o sua identidade para o centro da geração que fornece com a sua assinatura. Na fase de verificação do usuário, os usuários que desejam se comunicar desafiar uns aos outros antes de gerar as chaves de sessão na fase de troca de chaves. Nesta abordagem, a chave pública é gerada com base na identidade do dispositivo e a chave privada é gerada por uma terceira parte de confiança chamado um gerador de chave privada (KGC).

As principais vantagens do IBC (Criptografia baseada em identidade) são o processo de gerenciamento de chaves simples e redução do custo de armazenamento de memória em comparação aos métodos tradicionais de chaves públicas. Os dispositivos devem manter apenas os parâmetros PKG e não a chave pública de todos os outros dispositivos. Em IBC cada nó é capaz de descobrir a chave pública do outro nó sem trocar quaisquer dados. Além disso, um par de nós A e B é capaz de calcular um parelhamento de chave pré-compartilhada K AB de forma

não interativa. Esta chave pré-compartilhada pode ser usada em esquemas de criptografia para autenticação e protocolos de autenticação de acordo com a chave.

O fator mais importante de criptografia baseada em ID é o gerenciamento de chaves baseado em identidade. Isso afeta diretamente o desempenho e a segurança do algoritmo de criptografia. Existem vários esquemas baseados em chaves de identidade para MANETs, bem como campos de aplicação que eles usam. O grande problema com esquemas baseados em ID é que a chave privada de todos os usuários devem ser conhecidas pelo KGC. Em redes convencionais este não é um problema, mas em MANETs em que o KGC deve ser distribuído ou emulado por uma entidade arbitrária, isso pode ser um grande problema. Ele também precisa de um canal seguro para a troca de chaves privadas com cada nó. Além disso, em esquemas baseados em ID acontece a falta de anonimato e preservação de privacidade, devido as chaves públicas serem diretamente derivadas da identidade dos nós. O esquema WAPI(*Wireless Authentication and Privacy Infrastructure*) [40] considera a autenticação de acesso para os terminais móveis nas redes heterogêneas 3G-WiFi. Este esquema de autenticação usa o protocolo de combinação lógica (PCL). O PCL suporta a combinação de protocolos de segurança e usa conceitos de padrão lógico. Entretanto, o esquema WAPI não oferece segurança contra ataque de repetição. O protocolo de autenticação LRA (*Lightweight Roaming Authentication*) [41] propôs uma autenticação para transição entre redes que oferece uma comunicação leve e anonimato no meio sem fio sem a participação de um servidor residencial. A prevenção do ataque de repetição pode falhar devido a reutilização dos números randômicos utilizados para rejeitar quadros repetidos. Além disso, não oferece segurança quando o ataque visa a negação de serviço do ponto de acesso.

3.3 Autenticação baseada em grupo

Controle de autenticação baseado em grupo consiste em uma chave única que atribui-se a um grupo de nós (dispositivos computacionais). Nesta abordagem, todos os membros do grupo contribuem para a formação da chave de grupo comum. Esta chave pode ser atualizada periodicamente ou apenas quando os membros do grupo mudarem. Neste esquema, duas árvores multicast funcionam em paralelo, chamada de árvore azul e vermelha, o que garante a tolerância a falhas no sistema. No caso de um enlace estar fraco, este substitui-se por outra árvore. A coordenadores de grupo, um nó de iteração da rede distribui o material de chave intermediária para os membros. Este nó também mantém a conexão de grupo em multicast. Todos os nós nesta abordagem possuem um certificado válido de uma configuração de rede. Isto implica que há uma infra-estrutura subjacente de chave pública necessária para gerenciar os certificados.

O controle de autenticação GHAP (*Group-based Handover Authentication*), proposto em [42], estabelece um mecanismo de autenticação baseado em grupo de handover para estações móveis correlacionadas em redes IEEE 802.16m. Este controle de autenticação transmite todo o contexto de segurança dos membros do grupo de handover para a estação base alvo usando o método SCT (*Security Context Transfer*) durante a primeira fase de autenticação handover do dispositivo móvel. O esquema pode resistir de maneira eficaz contra o ataque de efeito dominó existente nos esquemas SCT conhecidos.

A abordagem de autenticação GBHA *Group-based Handover Authentication*), proposta em [43], se baseia em grupo de handover para redes WiMAX. Este esquema transmite todos os contextos de segurança do grupo handover membros para o ponto de acesso alvo usando o SCT durante a primeira fase de autenticação handover.

A Figura 3.4 representa o funcionamento do esquema GBHA. Neste esquema o dispositivo móvel (UE) realiza primeiramente a autenticação na torre de comunicação WiMAX. Deste forma, para o UE efetuar a transição, as antenas trocam informações sobre o dispositivo

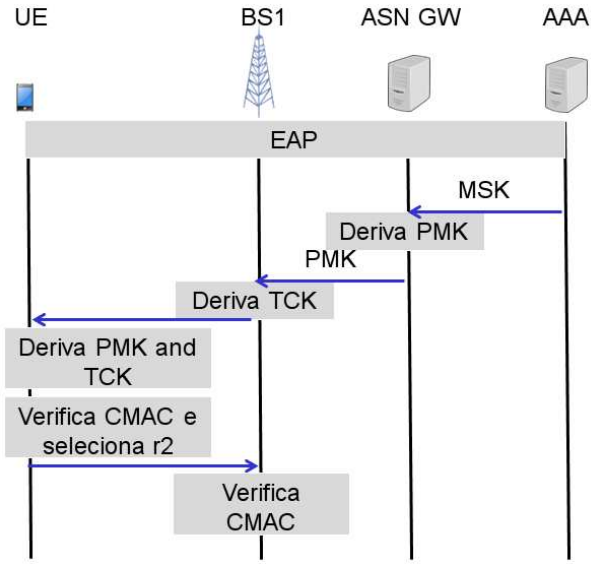


Figura 3.4: Inicialização de autenticação do esquema GBHA

para permitir que este efetue a autenticação. Ao contrário dos sistemas convencionais de SCT, o contexto de segurança não é utilizado como o material de chave para derivar a nova chave de sessão, mas serviu como uma chave simétrica da mensagem baseado no CMAC para processar a autenticação mútua para o protocolo de duas trocas de mensagens. O dispositivo móvel só fornece um pseudônimo em vez de sua identidade real na fase de autenticação inicial e muda seu pseudônimo em cada fase de autenticação para que ele possa proteger a privacidade de identidade dos dispositivos e evitar que o adversário trace sua rota de movimento.

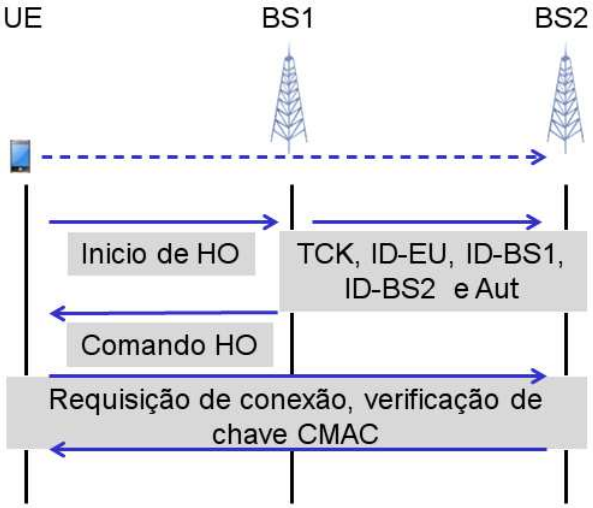


Figura 3.5: Autenticação de Handover do esquema GBHA

Após a fase inicial de autenticação o esquema de autenticação esta apto para efetuar a autenticação durante o processo de transição. A Figura 3.5 ilustra a fase de inicialização do esquema. O GBHA utiliza-se de comunicações entre as antenas da rede WiMAX para efetuar a autenticação do diposisitivo móvel. Basicamente, as torres de acesso se comunicam para que a autorização de autenticação para o dispositivo móvel seja liberada. Após a confirmação das torres de comunicação, este dispositivo pode enviar sua identificação com respectivas chaves para obter acesso durante o serviço de handover.

3.4 Autenticação baseada em emparelhamento

Neste esquema, quando um novo nó quer se juntar a rede, ele vai primeiro ser autenticado pelos seus nós vizinhos antes de todos os nós do agrupamento poderem formar uma base limiar de chave privada de geração de serviço em que um nova chave mestra pública deve ser gerada para o sistema de criptografia e uma nova chave mestra secreta compartilhada entre os nós. O novo nó pode obter sua chave privada pessoal combinando as ações de chaves privadas de cada um dos nós t que formaram a geração de serviço. Além disso, a chave pessoal pública gerada tem como base a identidade do próprio dispositivo.

Neste projeto, foi proposto um protocolo de autenticação handover chamado PairHand, que usa criptografia baseada emparelhamento para garantir processo de transferência e reduzir as despesas gerais de comunicação e computação das entidades envolvidas. Além disso, ele requer apenas duas trocas de mensagens entre um UE e um AP, e não precisa para transmitir ou verificar qualquer certificado como em sistemas de criptografia de chaves públicas tradicionais. Além disso, um sistema de verificação de assinatura em que cada AP pode verificar simultaneamente várias assinaturas recebidas. PairHand usa criptografia baseada em emparelhamento para garantir processo de transferência e para atingir alta eficiência.

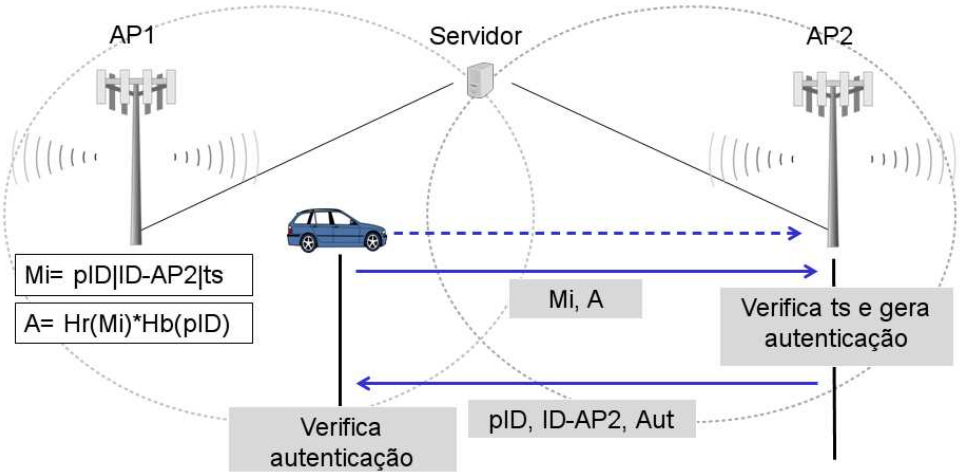


Figura 3.6: Autenticação do esquema PH

Os esquemas PairHand (PH) [14] e HashHand [7] usam criptografia baseada em emparelhamento para garantir processo de transferência e para atingir alta eficiência. A Figura 3.6 ilustra o funcionamento do esquema PairHand. Ao projetar PairHand, os autores n ao utilizaram nenhuma das primitivas criptográficas existentes, como a assinatura cega, assinatura anel e técnicas de assinatura em grupo. A técnica adotada pelos autores foi de preservação de privacidade baseado em pseudônimos. Os dispositivos móveis geralmente têm grande capacidade de armazenamento, tornando o pré-carregamento de um grande conjunto de pseudônimos do servidor de acesso viável. Apesar disto, a obtenção dos quadros contendo informações sobre as chaves o pseudo ID podem ser obtidas por um atacante e aplicadas em um ou mais pontos de acesso.

3.5 Outras estratégias

PPS [44] apresenta um esquema de transferência com base em pré-autenticação usando criptografia de chave simétrica para facilitar o handover possibilitando maior rapidez e segurança

para redes WiMAX móveis. O esquema é formalmente verificado por meio de lógica BAN para provar a sua capacidade de atingir as metas de um esquema de autenticação de segurança. HACH [45] usa credenciais baseadas em chameleon hash. Os principais desafios para a autenticação de entrega são para fornecer uma segurança robusta e eficiência. A idéia principal ideia é que as credenciais foram geradas usando a função hash resistente à colisão proporcionar uma troca de chaves autenticadas Diffie-Hellman efêmera apenas entre um nó móvel e um ponto de acesso sem se comunicar com um servidor de autenticação sempre que ocorre uma autenticação handover.

O esquema FHA [46] apresenta um mecanismo de autenticação de entrega rápida com base na credencial para IEEE 802.16m. O bilhete credencial de estação móvel é emitido pela estação de base de acesso usando uma chave de grupo de múltiplas estações base durante a autenticação inicial. Quando a estação móvel efetua o serviço de transição de uma estação base para outra, ele pode mostrar sua credencial para a estação base destino e esta autenticar a estação móvel sem se comunicar com qualquer outro terceiro.

PBA [47] mostra um esquema de autenticação para transmissão eficiente chamado de autenticação baseada em Predição (PBA). O PBA tem a capacidade de se defender contra ataques de negação de serviço baseados em computação, mas também de resistir a perdas de pacotes causados pela alta mobilidade de veículos. Em contraste com a maioria dos esquemas de autenticação existentes para VANETs, o PBA é um esquema eficiente e leve, uma vez que é construído principalmente em criptografia simétrica. Para reduzir ainda mais o atraso de verificação para algumas aplicações de emergência, o PBA explora a capacidade do veículo remetente para prever futuras balizas antecipadamente. Além disso, para evitar ataques de memória baseados em DoS, o PBA armazena apenas códigos encurtados de autenticação de mensagens de assinaturas sem diminuir a segurança.

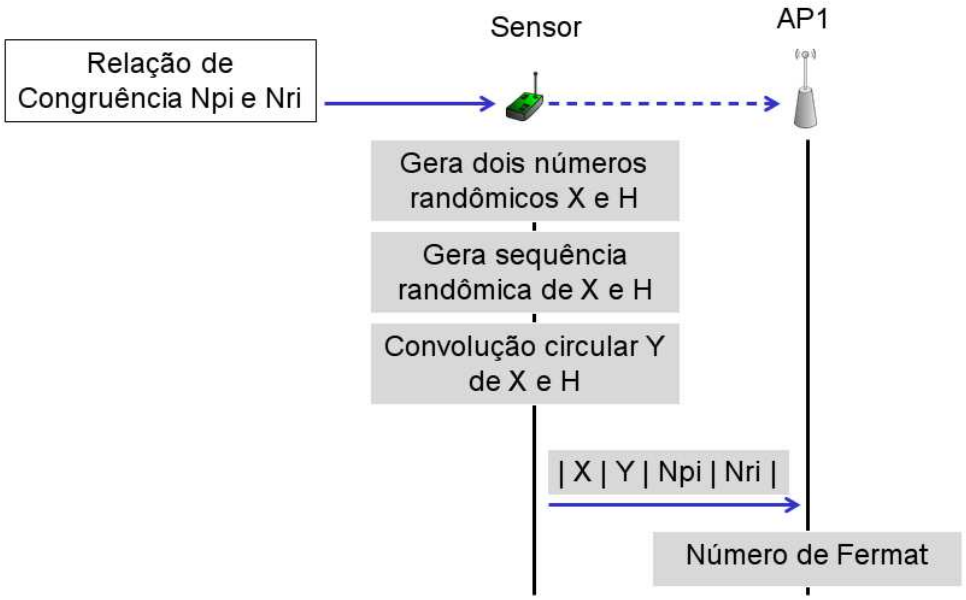


Figura 3.7: Autenticação do esquema LAP

O controle de autenticação LAP em [48] propôs um protocolo seguro com base nos conceitos da teoria dos números e equações de congruência que foi introduzida para fornecer autenticação entre os nós de sensores e servidores de banco de dados em uma rede sem fio. O protocolo proposto utiliza a transformação do número Fermat e partes do teorema chinês para permitir a comunicação segura. O protocolo usa seu próprio algoritmo de criptografia e descrip-

tografia para reduzir a complexidade computacional envolvido em algoritmos existentes. Para preparar a autenticação no cenário de autenticação de sensores primeira mente um dispositivo computacional faz a gerência das chaves para cada estação base e sensor da rede. Esta gerência de chaves ocorre através da distribuição de números primos gerados randomicamente. Estes valores de números primos são armazenados nos sensores. Quando um sensor precisa se conectar a um ponto de acesso, ele efetua cálculos a partir destes números primos gerando uma sequência randômica e convolução circular. Com os valores obtidos o sensor envia para o ponto de acesso que realiza o calculo de Fermat. Se os resultados corresponderem, o sensor se autentica com o ponto de acesso

3.6 Vulnerabilidades das técnicas

A partir das vulnerabilidades detectadas nas técnicas de autenticação existentes foram definidos os requisitos necessários para um sistema de autenticação robustos a ataques de repetição de identidades. Os requisitos consistem em segurança e desempenho. A confidencialidade e disponibilidade são requisitos de segurança que devem ser garantidos contra o ataque de repetição. Os requisitos de desempenho da rede correspondem a interoperabilidade, a gerência simples de chaves, o tempo de autenticação e o custo computacional. Estes requisitos são fundamentais para que o serviço de autenticação não afete a transparência do serviço de transição.

Tabela 3.1: Requisitos desejados para um esquema de autenticação em RHSF

TRABALHO	ABORDAGEM	PRIVACIDADE	DISPONIBILIDADE	INTEROPERABILIDADE	FUNC. SIMPLES	TEMPO	CUSTO COMP.
IACPK [40] (2012)	Cript. ID	Fraca				Médio	Médio
UHA [17] (2012)	Cript. ID	Média		Sim	Sim	Médio	Médio
GBHA [41] (2012)	Grupo de chaves	Forte				Médio	Pesado
GHAP [43] (2012)	Grupo de chaves	Forte				Médio	Pesado
PH [42] (2013)	Emp. bilinear	Fraca			Sim	Baixo	Médio
HH [14] (2012)	Emp. bilinear	Fraca			Sim	Baixo	Médio
WAPI [40] (2012)	Cript. ID	Fraca		Sim		Médio	Médio
LRA [41] (2012)	Cript. ID	Fraca		Sim		Médio	Médio
LAP [48] (2014)	Out. estrat.	Fraca				Baixo	Leve
PPS [44] (2012)	Out. estrat.	Fraca				Elevado	Pesado
HACH [45] (2010)	Out. estrat.	Fraca				Médio	Pesado
FHA [46] (2010)	Out. estrat.	Fraca				Baixo	Pesado
PBA [47] (2015)	Out. estrat.	Fraca				Elevado	Pesado

A Tabela 3.1 sintetiza os trabalhos existentes na literatura de controle de autenticação e os requisitos de necessários para RHSF. Nela, os requisitos estão organizados em duas perspectivas de desempenho e segurança. A primeira perspectiva abrange requisitos de segurança que são a privacidade e a disponibilidade. A privacidade nesse contexto, avalia a capacidade do esquema proteger a mensagem de autenticação. A disponibilidade consiste da manutenção da conectividade do dispositivo móvel diante de ataques contra a autenticação.

A segunda perspectiva de requisitos estão relacionadas ao desempenho da rede que são a interoperabilidade, funcionamento simples, tempo e custo computacional. A interoperabilidade compreende o funcionamento do esquema de autenticação em redes de tecnologias diferentes. O funcionamento simples representa a complexidade do gerenciamento das identidades e chaves dos dispositivos móveis. O tempo expressa o tempo levado para executar o serviço de autenticação. O custo baseia-se no custo de processamento do dispositivo móvel para execução do serviço de autenticação.

De acordo com a tabela, os trabalhos existentes na literatura não atendem a todos os requisitos necessários para sistemas de detecção de ataque de repetição de identidades nas RHSF. As estratégias criticadas anteriormente apresentam soluções adequadas para contextos diferentes, porém inspiradoras para um nova estratégia de autenticação em redes heterogêneas. Assim, a adaptação das ideias para um contexto de redes heterogêneas pode resolver diversos problemas de desempenho e solucionar ataques de autenticação.

A adaptação das estratégias consiste na utilização de um controle unificado onde as redes poderiam trocar informações entre identidades e chaves através de uma entidade central de autenticação. Isto permite a criação de mecanismo de autenticação mais resistentes a ataques contra a identidade dos dispositivos e com isso o acesso indevido. Além disso, estabelecer regras através de fases para inicialização da autenticação dos dispositivos móveis nas redes e a autenticação no processo de *handover* vertical auxília a obtenção de um controle de acesso mais robusto.

3.7 Resumo

Este capítulo apresentou as técnicas e soluções de autenticação propostas da literatura para redes heterogêneas que consideram a possibilidade de handover durante a mobilidade do usuário. As técnicas apresentadas consistem das abordagens baseadas em identidade, grupo e emparelhamento. Além disso, neste capítulo foi realizada uma breve contextualização dos métodos de autenticação mostrando as vantagens e desvantagens.

Capítulo 4

ARARAS: Esquema de autenticação contra repetição de identidades em RHSF

Este capítulo apresenta um esquema para assegurar a segurança do serviço de autenticação contra ataques de repetição de identidades que ocorram no *handover* sobre redes heterogêneas sem fio. A Seção 4.1 descreve uma visão geral do esquema proposto, destacando suas características, seus objetivos, e suas fases. A Seção 4.2 detalha o modelo da rede assumido, bem como a composição da RHSF. A Seção 4.3 mostra o perfil do ataque de repetição considerado neste trabalho. A Seção 4.4 descreve em detalhes os componentes do sistema e suas fases de atuação. Por fim, a Seção 4.5 apresenta a atuação do mecanismo diante de um ataque de repetição.

4.1 Visão geral

O esquema proposto chamado ARARAS (**A**utenticação **R**esistente a **A**taques de **R**epetição de Identid**A**des em Rede**S** Heterogêneas), tem como objetivo auxiliar o processo de autenticação na transição de conexões de forma a resistir ao ataque de repetição de identidades (RI) nas redes heterogêneas sem fio. No esquema ARARAS, o serviço de autenticação possui um controle de mensagens que suporta a detecção de identidades repetidas. Ademais, as redes trocam informações acerca dos dispostivos e suas respectivas identidades independente do tipo de tecnologia de rede empregado no ambiente. Para isso, o requisito do ARARAS consiste da sobreposição das redes.

O ARARAS atende à três princípios para cumprir o objetivo de proteger as redes. O primeiro se relaciona à prevenção do ataque de repetição de identidades no processo de *handover*. Desta forma, o ARARAS usa as fases de inicialização e autenticação, juntemente com o mecanismo de proteção. O segundo princípio compreende a unicidade da autenticação para verificar o tempo das mensagens e distribuir informações acerca da identidades dos dispositivos móveis. Por fim, o terceiro princípio visa a otimização da autenticação.

O arcabouço do esquema ARARAS possui duas fases e um mecanismo de proteção. As fases de autenticação representam uma maneira unificada de efetuar a autenticação nas RHSFs [49]. A unificação da autenticação propicia um melhor gerenciamento de identidade e distribuição de chaves entre as tecnologias de redes. A primeira fase chamada de inicialização consiste da requisição de autenticação de um dispositivo móvel para um ponto de acesso que atribui a ele a identidade e chaves. Essa fase acontece entre o dispositivo móvel e a rede de maior sobreposição de abragência sem fio. A segunda fase proporciona o serviço de autenticação na transição nas redes heterogêneas. Nessa fase, o dispositivo móvel pode se autenticar com as redes através da identidade e chaves obtidas na fase de inicialização do esquema ARARAS. Essas

fases apoiam uma gerência simples de autenticação contribuindo para prevenção de ataques independente do tipo de tecnologia de rede.

O esquema ARARAS conta ainda com o mecanismo de proteção de mensagens de autenticação que exerce a análise das mensagens recebidas durante as fases de autenticação com objetivo de rejeitar mensagens provenientes de ataques. Esse mecanismo presente no esquema proposto analisa as mensagens partindo de três princípios. Os princípios considerados possuem relação com o tempo de mensagem, quantidade de mensagens recebidas e a verificação da identidade que ocorre na infraestrutura das redes heterogêneas.

4.2 Modelo da rede

As redes heterogêneas agregam diversos dispositivos computacionais que possuem características e funcionalidades diferentes [50]. Esses dispositivos computacionais consistem de dispositivos móveis (nós), pontos de acesso (AP) e o autenticador que pode ser do tipo local para as redes com baixo alcance de transmissão e central para redes com grande alcance de transmissão de dados, como mostra a Figura 4.1. Assim, o ambiente da RHSF compreende a heterogeneidade dos seus dispositivos computacionais e que precisam estabelecer comunicações. O modelo de rede considerado nesta proposta possui como componentes, os pontos de acesso e dispositivos móveis (nós). As redes heterogêneas são compostas por um conjunto de redes H = $\{r_1, r_2, r_3, ..., r_n\}$, tal que $r_n \in H$, onde r significa cada rede presente no conjunto de redes heterogêneas H. Essas redes podem possuir um ou mais APs, tal que cada rede possui um conjunto de pontos de acesso AP onde AP= $\{ap_1, ap_2, ap_3, ..., ap_n\}$ tal que $ap_n \in AP$, onde ap representa um ponto acesso específico dentro do conjunto de ponto de acesso AP em uma rede. Cada rede possui um conjunto de dispositivos móveis N = $\{n_1, n_2, n_3, ..., n_n\}$ tal que $n_n \in N$ conectados por um ou mais pontos de acesso. A conexão efetuada por um nó em uma rede é representada por $C_w^{ap_i, r_j}$, onde a conexão C_w, ap_i o ponto de acesso no qual o nó obtem conexão e r_i a rede. Quando o nó se autentica, o autenticador local ou global fornece uma identidade I= $\{i_1, i_2, i_3, ...i_n\}$, tal que $r_n \in I$. Cada nó conectado na rede possui uma identidade, logo, IR = $\{(i_1, n_1), (i_2, n_2), (i_n, n_n)\}$, onde IR representa as identidades presentes na rede e (i_n, n_n).

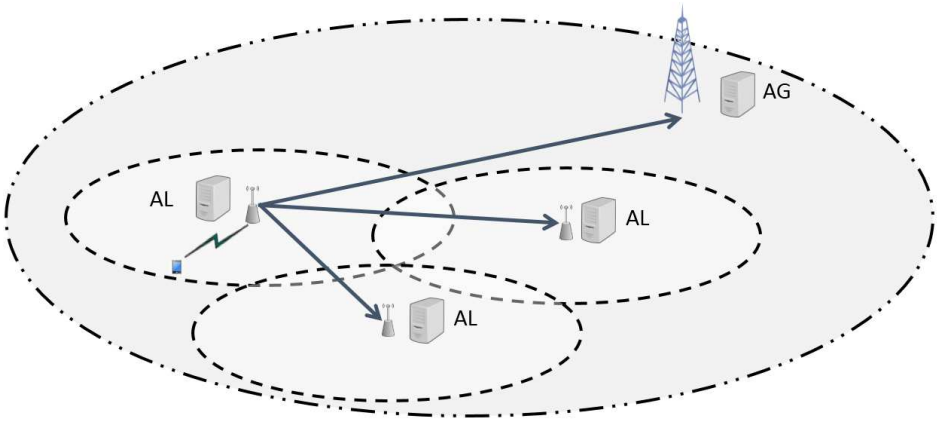


Figura 4.1: Modelo da rede

A comunicação entre os dispositivos móveis e o ponto de acesso acontece no meio sem fio. Os pontos de acesso estão ligados ao autenticador da rede através de cabos. Essa conexão cabeada possui um canal seguro que impede que ocorra um ataque durante a comunicação. A comunicação entre redes de diferentes tecnologias ocorre através do meio sem fio utilizando um

canal de comunicação seguro. Isso impede ataques de comunicação entre as redes. Em redes do tipo WWAN e WLAN, a comunicação dos núcleos da rede acontece através do protocolo de comunicação seguro ePDG (*Evolved Packet Data Gateway*). Esse protocolo garante a comunicação confidencial entre as entidades de cada núcleo da rede. A troca de informações entre as redes tem como objetivo auxiliar a gerência de identidade e de chaves.

4.3 Comportamento do ataque de repetição de identidades

O ataque de repetição de identidades considerado nesta proposta usa identidades roubadas para obter acesso às redes. Assim, os atacantes utilizam de meios como a captura dos quadros e análise das mensagens de autenticação no meio sem fio. O ataque acontece no momento de execução do serviço de autenticação do dispositivo móvel para conseguir acesso em alguma rede. Ao obter a mensagem de um dispositivo móvel o atacante pode efetuar os ataques com a identidade capturada e assim replicá-la.

O ataque funciona através do envio da repetição da mensagem com a identidade que foi roubada efetuando a personificação do dispositivo legítimo em um ponto de acesso ap_1 ou para um outro ponto de acesso vizinho ap_i. O ataque de repetição de identidades engana o dispositivo móvel que envia informações ao atacante como se fosse um ponto de acesso. Dessa forma, o atacante obtém informações do dispositivo móvel. A Figura 4.2 apresenta o instante em que o dispositivo móvel legítimo realiza o *handover* vertical entre as redes. O atacante efetua a captura das identidades quando o dispositivo móvel realiza serviço de autenticação no processo *handover* vertical e realiza a replicação obtendo acesso não autorizado.

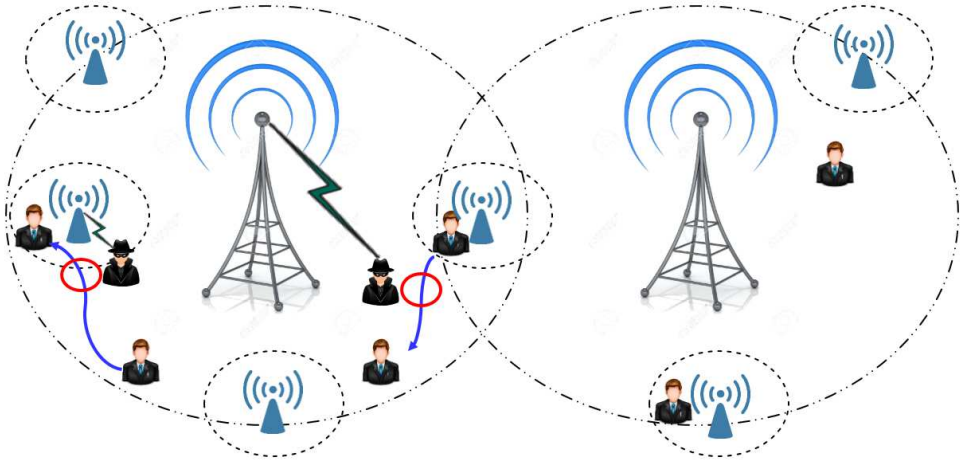


Figura 4.2: Modelo do ataque

O ataque RI pode personificar um ou mais nós entre os pontos de acesso das redes heterogêneas. Dessa maneira, um atacante pode capturar um conjunto de identidades de qualquer nó $N_i^{R_i,ap_i}$ que se conecte a uma rede por um ponto de acesso i, I = $\{n_1, n_2, n_3, ..., n_i\}$ tal que $n_i \in N$ onde N é conjunto de nós que se conectaram a um ponto de acesso de uma rede em um período de tempo. Isto exige da autenticação uma forma de impedir que a personificação ocorra em outras redes presente no ambiente.

4.4 Descrição dos Componentes do ARARAS

O controle de autenticação proposto compreende fases que são a inicialização de autenticação e autenticação de *handover*, e o mecanismo de proteção. A primeira fase demanda a autenticação do dispositivo móvel para obter a identidade e as chaves. A segunda fase representa o uso da identidade e chaves obtidas pela fase anterior para efetuar o *handover* vertical entre as redes de forma unificada. O mecanismo de proteção possui três módulos que auxiliam na prevenção de ataque de repetição após recebimentos de quadros. Essas fases juntamente com o mecanismo trabalham em conjunto a fim de realizar uma autenticação segura contra o ataque RI. As próximas subseções descrevem as duas fases e o mecanismo.

4.4.1 Inicialização

A fase de inicialização de autenticação tem o objetivo de efetuar uma conexão segura para o usuário do dispositivo móvel. Essa autenticação acontece através de um gerenciador de chaves central que auxilia o controle de acesso nas redes. Esse gerenciador central distribui as identidades e as chaves para os dispositivos computacionais presentes nas redes. Com essas chaves o usuário pode se autenticar nas demais redes de forma unificada. Nesta proposta, as tecnologias de redes consideradas correspondem à redes WWAN e WLAN (LTE e a WiFi/802.11). O autenticador central se encontra no EPC (*Evolved Packet Core*) da rede LTE. O EPC integra as redes WiFi com o autenticador para a distribuição de chaves. Dessa forma, um esquema criptográfico deve ser utilizado para auxiliar a distribuição de chaves criptográficas para os dispositivos das redes. Na comunicação dos dispositivos móveis e entidades da redes, utiliza-se um mecanismo de proteção contra o ataque RI, que é detalhado na Seção 4.5.

A gerência de chaves baseiam-se nas chaves públicas (Ppub) e privadas (Ppriv) utilizadas para autenticar os dispositivos móveis nas RHSF. Além disso, um número aleatório é utilizado para gerar as chaves dos dispositivos. Ainda na gerência de chaves, que ocorre no autenticador central, ocorre a distribuição de chaves e identidades dos dispositivos móveis entre os autenticadores das outras redes para proteger contra ataques que podem acontecer na fase de inicialização.

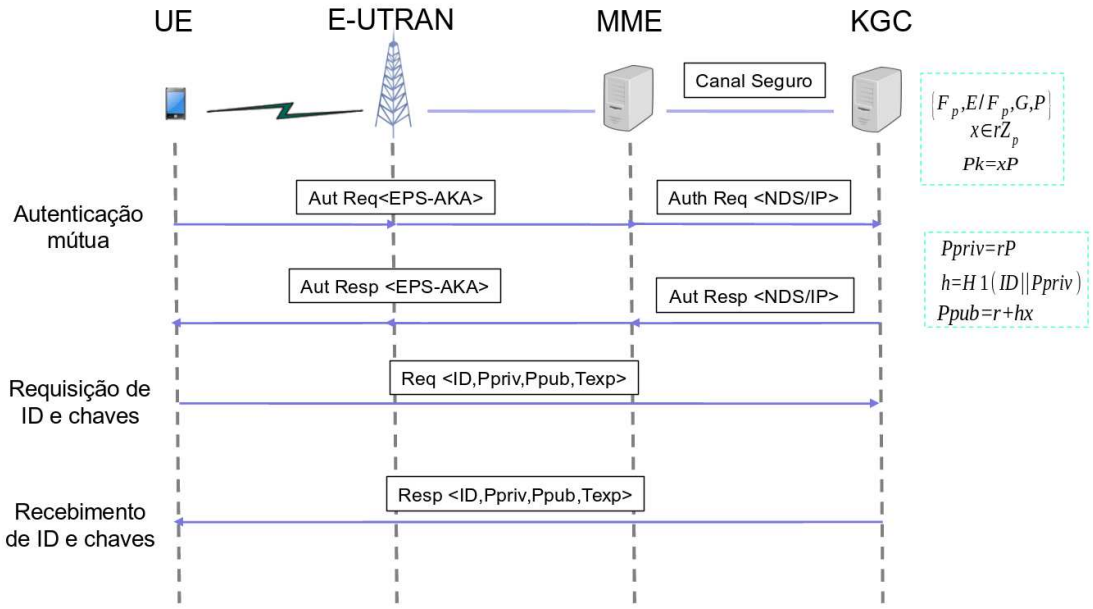


Figura 4.3: Inicialização de autenticação

A Criptografia Baseada em Emparelhamentos (*Pairing Based Cryptography*) possibilita o projeção e a utilização de esquemas criptográficos. Seja G um grupo cíclico aditivo e GT um grupo cíclico multiplicativo de mesma ordem q. O grupo G é um conjunto que possui as propriedades de identidade e associação. O parâmetro P é um gerador arbitrário de G e aP indica o P posicionado para ele mesmo. Um mapeamento bilinear ê corresponde à ê $= G*G \rightarrow GT$ que satifaz as regras de bilinearidade, não degenerar e computabilidade. A bilinearidade corresponde a regra $\hat{e}(aP, bQ) = \hat{e}(P,Q)^a b$, onde $P, Q \in G$ e $a, b \in Z * q$. O valor $Z * q$ corresponde à $Z * q = \{\rho | 1 \leq \rho \leq q - 1\}$. O mapeamento bilinear não pode ser degenerado, logo, $e(P,P) \neq 1$. A regra de computabilidade consiste de um algoritmo de eficiência que calcula $\hat{e}(P,Q)$ para qualquer $P, Q \in G$.

Na fase de inicialização da autenticação alguns procedimentos são seguidos de acordo com a distribuição de identidades e chaves. Dessa forma, o dispositivo móvel (UE) requisita por conexão em uma rede do tipo WWAN, primeiramente o gerenciador central efetua a autenticação do dispositivo através do chip de identificação. Através dessa autenticação, uma identidade para o UE é gerado juntamente com as chaves pública e privada (chave assimétrica) para acesso entre as redes heterogêneas. O UE pode requisitar autenticação na rede do tipo WLAN para criação de identidade e chaves. Nesse caso, essa identidade e chaves devem ser armazenadas no gerenciador central das redes para que possa ser associado a outros tipos de redes, no caso desta proposta a rede do tipo WWAN. A associação ocorre quando o UE requisitar em outro momento a autenticação com o outro tipo de rede através da relação entre as identidades e chaves com a identidade do chip do dispositivo.

Seja G um grupo cíclico aditivo e GT um grupo cíclico multiplicativo de mesma ordem q e seja P um gerador randômico de G, $G * G \rightarrow GT$ originando um mapa bilinear. Assim, o gerenciador de chave central escolhe um número aleatório $s \in Z * q$ como a chave mestra e calcula a chave pública correspondente $pub = sP$. Além disso, duas funções hash de segurança $H1$ e $H2$ são determinadas, onde $H1 : \{0,1\}* \rightarrow G$ e $H2 : \{0,1\}* \rightarrow Z * q$. No final, o gerenciador central publica os parâmetros de autenticação das redes $\{G, GT, q, P, pub, H1, H2\}$ e mantém a chave privada secretamente. Para cada ponto de acesso, o gerenciador de chaves central calcula $H1(IDAP)$ como a chave pública e $sH1(IDAP)$ como a chave privada. Assim, esse gerenciador envia as chaves para o ponto de acesso (AP), onde $IDAP$ representa a identidade de cada AP.

O exemplo de funcionamento é mostrado na Figura 4.3 utilizando como instância a rede LTE. O usuário através do dispositivo móvel requisita conexão com a torre E-UTRAN que envia a requisição para o centro de processamento da rede LTE chamado de EPC. No EPC, as entidades responsáveis pela autenticação do usuário são o servidor de gerência de mobilidade (MME) e o servidor de autenticação (AAA). O servidor AAA fornece a gerência de criação e distribuição de chaves para cada dispositivo móvel. Assim. o dispositivo móvel recebe sua identidade da rede e o par de chaves para o acesso entre as redes. Ao receber as chaves, o dispositivo móvel se autentica com a rede LTE.

4.4.2 Autenticação no handover

A fase de autenticação na transição de redes, ou *handover*, tem o propósito de prevenir do ataque de repetição. Nesta fase, o dispositivo móvel utiliza as chaves pública e privada para efetuar a autenticação durante o *handover* vertical entre redes heterogêneas. A chave pública e privada (assimétrica) fornece proteção contra o ataque RI na rede durante a requisição do dispositivo móvel para o ponto de acesso. A chave assimétrica garante que apenas o dispositivo legítimo possa descriptografar a mensagem de autenticação através da chave privada (chave

secreta). Apesar disso, a captura de quadros acontece de acordo com as mensagens do dispositivo móvel e ponto de acesso. A captura e replicação de quadros do ponto de acesso pode ser efetuada representando o ataque RI no dispositivo do usuário. Para prevenir esse ataque um mecanismo deve atuar para verificar os quadros.

A autenticação dos dispositivos móveis durante o *handover* é expressa por Aut(ni)=Nap,a(ni)+Pi(AP(apj)->A(ai)), onde Aut representa o autenticador de um nó i, Nap,a(ni) o nó conectado em outro AP e autenticador, Pi a probabilidade de autenticação ocorrer, AP(api) o conjunto de pontos de acesso e A(ai) o conjunto de autenticadores.

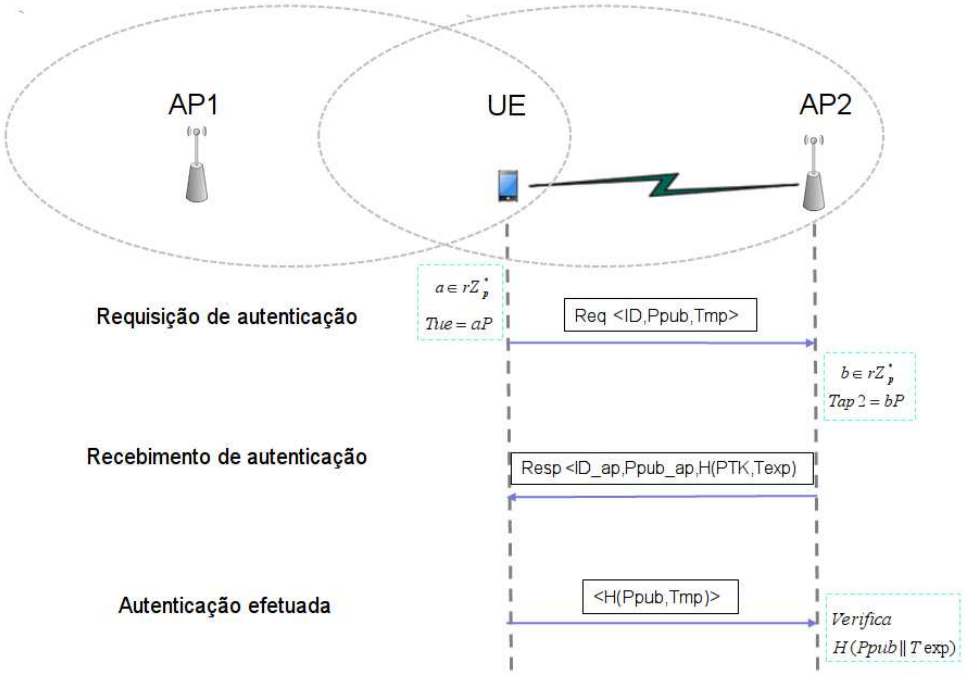


Figura 4.4: Autenticação de *Handover*

Cada AP transmite sua identidade como parte das mensagens de autenticação que são periodicamente transmitidas para declarar a existência de serviços. Um UE segue o protocolo de autenticação de entrega quando um AP está dentro de seu alcance de comunicação direta. O dispositivo móvel possui sua identidade e chaves criptografadas. A mensagem de autenticação então é enviada para o ponto de acesso, sendo a mensagem $M = (pID|IDAP|ts)$, onde pID representa a pseudo-identidade do UE. O dispositivo móvel calcula a assinatura $A = H2(M) * sH1(pID)$, onde um *timestamp* ts é adicionado para auxiliar a prevenção de ataques de repetição e a mensagem indica uma operação de concatenação. Dessa forma, todas as entidades da rede preservam a sincronização de tempo de mensagem através de um mecanismo de sincronização de tempo. Em seguida, o UE envia mensagens *unicast* de solicitação de acesso $\{Mi, A\}$ ao AP. Desse modo, o UE calcula a chave compartilhada simétrica com $AP : Ki - 2 = \hat{e}(sH1(ipID), H1(IDAP))$. Após a recepção da $\{M, A\}$, o AP efetua os procedimentos de verificação através do mecanismo de proteção e efetua suas tarefas de resposta de autenticação. Os selos de tempo ts são verificados para auxiliar na prevenção do ataque de repetição. O tempo de envio incluído no pID auxilia a verificação do tempo de expiração da mensagem do serviço de autenticação. Através da atribuição dos parâmetros realizada pelo gerenciador central, o AP analisa se a assinatura A possui validade se $\hat{e}(Ai, P) = e(H2(M) * H1(pID), pub)$. Então, $\hat{e}(A, P) = \hat{e}(H2(M) * sH1(pID), P) = \hat{e}(H2(M) * H1(pID), sP) = \hat{e}(H2(M) * H1(pID), pub)$. O AP calcula ainda $K2 - i = \hat{e}(H1(pID), sH1(IDAP))$. Os valores são analisados sendo $K2 - i = \hat{e}(sH1(pID), H1(IDAP))$

$= \hat{e}(H1(pID), H1(IDAP))$ $s = \hat{e}(H1(pID), sH1(IDAP)) = K2 - i$. O AP gera um código de autenticação $Aut = H2(K - 2|pID|IDAP)$. Portanto, o AP envia as informações $\{pID, IDAP\}$ e *Aut* para o dispositivo móvel. Ao receber $\{pID, IDAP, Aut\}$, dispositivo móvel gera um código de verificação $H2(Ki - 2|pID|IDAP)$ e compara com *Aut*. Se as informações $\{pID, IDAP\}$ e *Aut* corresponderem, o dispositivo móvel certifica-se que o AP é legítimo e estabeleceu uma chave K compartilhada 2-i; caso contrário, dispositivo móvel rejeita a conexão com o ponto de acesso.

O desempenho do AP na verificação da assinatura é predominantemente composta por operações de multiplicação de emparelhamento. Dessa forma, o AP transmite com segurança a mensagens de autenticação $\{M, A\}$ para o dispositivo móvel. Ao receber essa mensagem, o gerenciador central pode encontrar a verdadeira identidade do dispositivo móvel de acordo com a pseudo-identidade na mensagem de autenticação M. Assim, essa estratégia proporciona uma privacidade de emparelhamento bilinear condicional. Cada AP transmite sua identidade como parte das mensagens de autenticação que são periodicamente transmitidas para declarar a existência de serviços.

A fase de autenticação de *handover* utiliza as chaves atribuídas pela inicialização para efetuar a autenticação de *handover* de forma única e transparente ao usuário móvel. A Figura 4.4 ilustra o funcionamento. O dispositivo solicita autenticação com o ponto de acesso destino enviando sua identificação chave pública e tempo da autenticação. O ponto de acesso destisno através do mecanismo verifica a validade e unicidade da mensagem recebida. Se a mensagem for autêntica, o dispositivo móvel se conecta a rede.

4.4.3 Mecanismo de proteção

O mecanismo de proteção tem o objetivo de prevenir a personificação de identidade do ataque RI em redes que estejam no alcance do atacante no momento da captura de quadros. Esse mecanismo atua no recebimento da mensagem de autenticação. Os módulos presentes no mecanismo de proteção são a verificação de tempo, verificação de quadros e atualização de conexão como mostra a Figura 4.5. O módulo de verificação de tempo analisa o recebimento da mensagem *Trec*. Essa análise sucede da diferença do tempo de mensagem de autenticação enviada pelo usuário *Texp*, tal que *Texp* é embutida no quadro de autenticação, e o tempo de recebimento *Trec*. Dessa forma, a diferença consiste de *Texp* - *Trec*. Esse módulo fornece a garantia de que a mensagem é única durante o período de tempo.

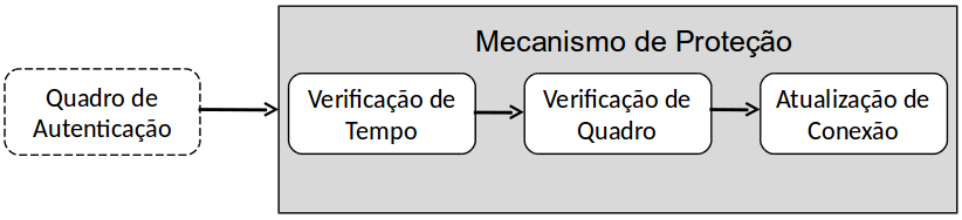


Figura 4.5: Mecanismo de Proteção

Cada quadro *qt* recebido pelo ponto de acesso possui sua identificação. A identificação é feita através da classificação de chegada de cada *qt*. Quando o quadro de autenticação *qt* chega no ponto de acesso, ele tem seus campos analisados e classificados como $qt = 1$, e então outros quadros que possuam os mesmos campos de autenticação serão recusados. Essa estratégia invalida o ataque de repetição que personifica um dispositivo móvel e ajuda a caracterizar se esse ataque essa sendo utilizado para efetuar negação de serviço. Para prevenir que o ataque seja

efetuado em redes vizinhas ao ponto de acesso em que o dispositivo móvel se conectou uma mensagem do ponto de acesso para os pontos de acesso vizinhos é enviada. Essa mensagem informa que o dispositivo móvel com uma identidade ID_i está conectado no ponto de acesso AP_i. Isso evita que o atacante propague a personificação em outras redes do ambiente sem fio.

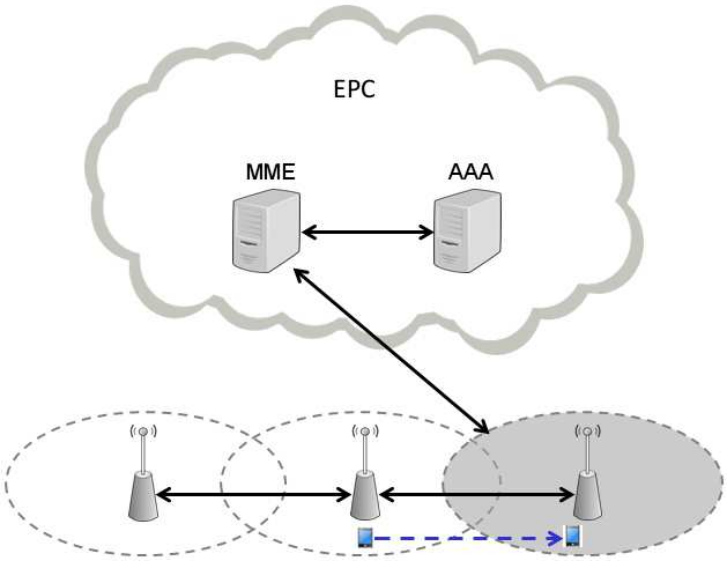


Figura 4.6: Atualização de Conexão

O envio das mensagens ocorre entre as redes através da verificação do conjunto de vizinhos. As redes mais próximas serão informadas sobre a identidade e conexões de um dispositivo móvel. Um conjunto de vizinho V onde $V = \{ap_1, ap_2, ap_3, ..., ap_i\}$ tal que $ap_i \in V$. Para que a redes estejam completamente informadas sobre a conexão do usuário, o ponto de acesso envia a mensagem para o centro da rede LTE, o EPC, sendo a quantidade de mensagens M enviadas do AP para atualização de conexão representada por M onde $M = V + 1$. O último módulo corresponde a atualização de informação sobre a conexão de um determinado dispositivo móvel apresentado na Figura 4.6. Esse módulo informa aos pontos de acesso vizinhos que o dispositivo móvel que possui uma identidade específica está conectado na rede.

4.5 Funcionamento do ARARAS diante do ataque RI

A Figura 4.7 ilustra o funcionamento do mecanismo ARARAS no instante em que um dispositivo móvel legítimo realiza o *handover* vertical e as redes se comunicam trocando informação sobre a autenticação. Assume-se uma redes heterogênea que consiste de três APs, denominados de AP 1, AP 2 e AP 3. Os dispositivos móveis representam o dispositivo de usuário legitimo, que busca fazer a transição da rede AP 1 e AP2, e os dispositivos dos atacantes, que executam o ataque no AP 1. No instante da transição do dispositivo do usuário legitimo da rede AP 1 à rede AP 2, o esquema ARARA então informa às redes vizinhas sobre esse dispositivo efetuando a troca de mensagens. A informação enviada ao AP 3 compreende a mensagem *Msg1* e ao AP 2, a *Msg2*, em ambas os valores corresponde ao ID, Ppub e ID_ap1. O valor ID consiste da identidade do dispositivo do usuário, valor Ppub representa a chave de acesso pública, e o valor ID_ap1 simboliza a identidade AP 1. O objetivo da troca da informação é impedir que a identidade de um dispositivo móvel legitimo seja usada para obter acesso não autorizado. Desta forma, o ataque repetição de identidades feito pelos dispositivos dos atacantes é anulado no AP 1.

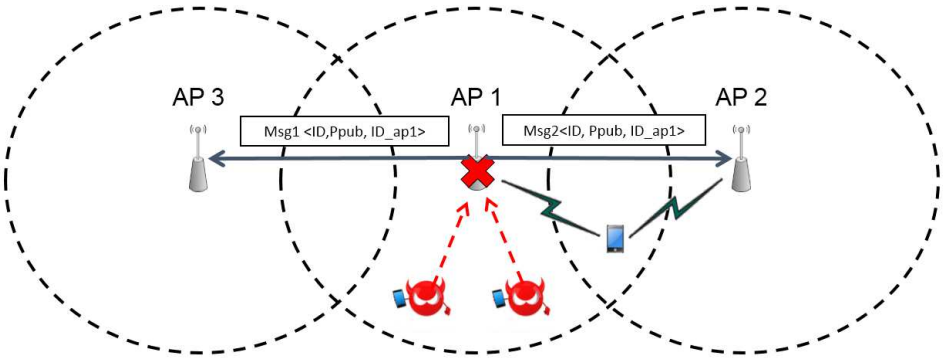


Figura 4.7: Comportamento do ARARAS diante do ataque RI

O atacante pode capturar a identidade de um ou mais dispositivos móveis e tentar obter o acesso não autorizado através da identidade capturada. A replicação de mensagem feita por um atacante pode acontecer em um ou mais pontos de acesso do conjunto AP. Contudo, em razão da troca de mensagens entre os APs a respeito dos dispositivos móveis conectados entre as redes, esse ataque é evitado pela rejeição da identidade vito que autenticadores reconhecem os dispositivos legítimos e suas posições de conexão nas RHSF. Assim, a partir da análise do funcionamento do ataque de repetição de identidades, o esquema ARARAS consegue detectar e anular as mensagens dos usuários maliciosos. Além disso, o esquema consegue suportar o serviço de autenticação seguro no *handover* vertical nas RHSF. Logo, o ARARAS atende aos requisitos de confidencialidade, disponibilidade, interoperabilidade, funcionamento simples, baixo tempo na execução da autenticação, e proporciona um custo computacional médio.

4.6 Resumo

Este capítulo apresentou a descrição do controle de autenticação resistente ao ataque de repetição de identidades considerando as características da rede que são o custo computacional, tempo de autenticação, interoperabilidade e funcionamento simples e características de segurança que são a privacidade e a disponibilidade do serviço de autenticação durante o processo de transição entre redes. O funcionamento do controle de autenticação compõem três fases, sendo a fase de inicialização responsável pela autenticação do usuário na rede segura 3GPP, a fase de autenticação de *handover*, que visa uma autenticação durante a transição entre redes de maneira segura e o mecanismo de proteção para verificação de validade dos quadros de autenticação.

Capítulo 5

Avaliação

Este capítulo apresenta uma análise de resistência do esquema de controle de autenticação ARARAS para prevenir o ataque de repetição na autenticação do processo de *handover* em redes heterogêneas. Essa avaliação mostra a eficiência em termo de segurança e apresenta uma comparação com o esquema UHA. A Seção 5.1 detalha a implementação dos esquemas ARARAS e UHA. A Seção 5.2 descreve o ambiente e cenário da simulação. A Seção 5.3 define os parâmetros e métricas usados para avaliação dos esquemas. Finalmente, a Seção 5.4 mostra e discute os resultados obtidos do cenário avaliado.

5.1 Implementação dos esquemas

Os esquemas ARARAS e UHA (*Unified Handover Authentication*) foram implementados no simulador NS-3, versão 3.24.1 utilizando a linguagem C ++ e a biblioteca Crypto++ na versão 5.63 para a implementação da criptografia baseada em emparelhamento e para o consumo energético a classe *energy model*. A implementação compreende além dos esquemas, o ataque de repetição de identidades (RI) efetuado por um dispositivo móvel malicioso e os módulos de redes de comunicação WiFi e LTE. Esses módulos representam as redes usadas frequentemente pelos aparelhos de telefonia celular modernos.

A biblioteca Crypto++ [51] oferece suporte na utilização de criptografia na comunicação entre as entidades das redes. O Crypto++ consiste de uma biblioteca que permite a implementação e a inserção de algoritmos de criptografia para simulação. Para a implementação e avaliação dos esquemas, foram necessários ajustes no código do simulador NS3 para compatibilidade com as bibliotecas. A Figura 5.1 representa o diagrama de classes do esquema ARARAS implementado no simulador NS3. As fases de inicialização e autenticação estão no módulo do esquema ARARAS. Nas entidades AP Global, Nó Móvel e AP Local estão as variáveis de funcionamento do esquema.

Dentre os esquemas de autenticação encontrados na literatura, o UHA mostrou-se mais efetivo e compatível com os cenários de redes heterogêneas. Esse esquema se adapta ao serviço de *handover* vertical entre as redes heterogêneas. O UHA também considera os módulos de redes WiFi e LTE e foi usado para comparação de segurança e desempenho.

5.2 Ambiente de avaliação

Os esquemas ARARAS e UHA foram avaliados num cenário urbano, onde assume-se as características de mobilidade do dispositivo móvel no ambiente. Logo, esses esquemas foram

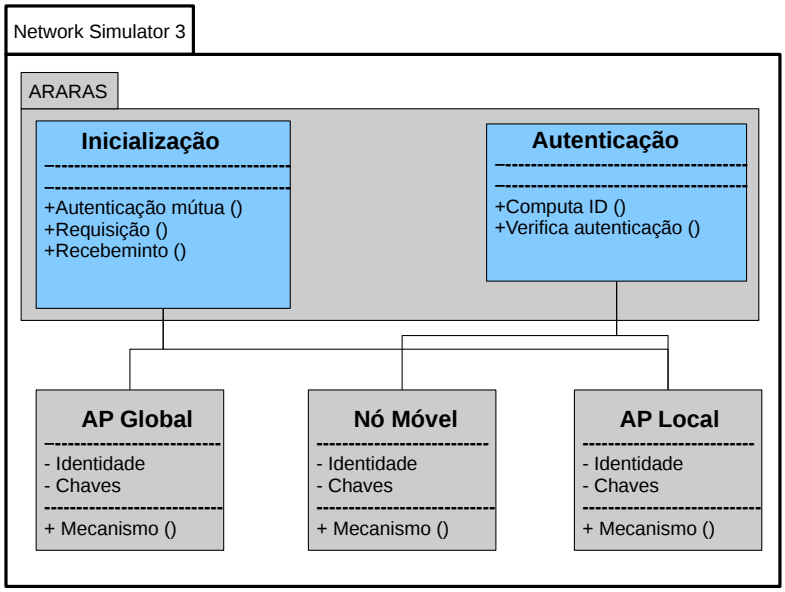


Figura 5.1: Diagrama de classe

expostos ao serviço de transição vertical e também aos ataques contra a identidade. Parte dos nós presentes no ambiente são maliciosos e capturam as mensagens de autenticação dos nós móveis.

O cenário de avaliação é composto de dispositivos com propriedades de mobilidade (nó móvel) e redes com áreas de cobertura de sinal sem fio sobrepostas. O ambiente metropolitano corresponde a um cenário urbano com uma área de 400m x 400m, representando o caminho que um usuário móvel faz quando se locomove de casa ao centro urbano. As redes presentes nessa área possuem sobreposição de transmissão de dados e compreendem 16 redes WiFi e 4 LTE. Isso permite ao usuário se mover e executar conexões através dos dispositivos. Os dispositivos dos usuários, que consistem dos nós móveis, se movimentam pelo ambiente de forma a alternar de conexão entre as redes, ou seja, executar o serviço de *handover*. Ao realizar o *handover* vertical entre as redes, o serviço de autenticação é requisitado. Os usuários maliciosos presentes nesse ambiente de sobreposição de redes heterogêneas captura as mensagens de autenticação a fim de replicar os quadros e obter acesso não autorizado.

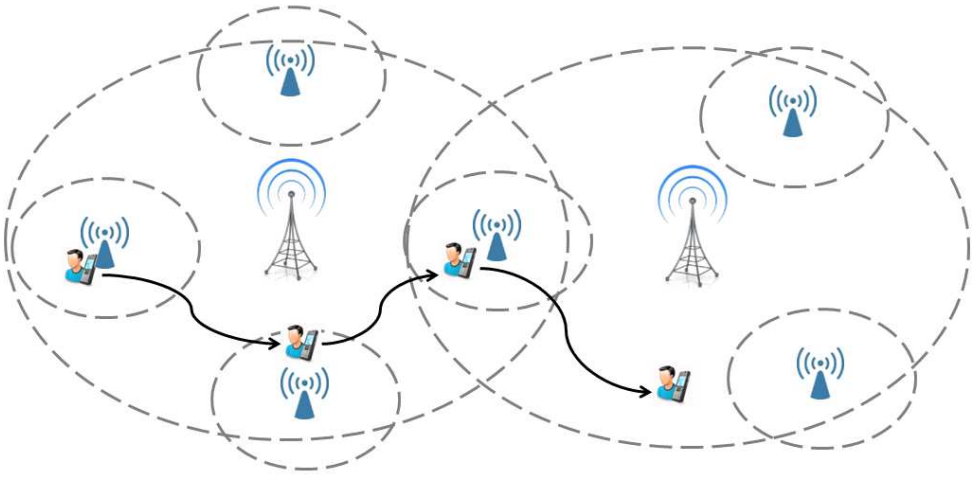


Figura 5.2: Cenário de Avaliação

Os pontos de acesso distribuídos no cenário foram configurados em 70 metros de alcance de transmissão para as redes WiFi e para LTE abrangem todo o cenário. Devido a diferença entre as tecnologias empregadas no cenário, a sobreposição de transmissão de dados das redes varia. As redes Wifi foram distribuídas pelo cenário de forma a manterem 2 redes vizinhas sobrepostas de mesma tecnologia. Além disso, cada rede WiFi possui sobreposição de transmissão com todas as redes LTE. As redes LTE permitem a sobreposição com todas as redes pois cobrem todo o cenário da simulação.

O cenário utilizado na avaliação representa um ambiente de centro urbano com redes sobrepostas que possuem longo e curto alcance de sinal sem fio. Nesse cenário representado pela Figura 5.2, os nós se movem no ambiente e utilizam o processo de transição de conexão nas redes sem fio. Logo, o serviço de autenticação prestará suporte ao processo de *handover* sempre quando for necessário a transição para outra rede. Os nós atacantes posicionam-se em partes do cenário onde existe grande sobreposição de redes. Dessa forma, esses nós efetuam uma grande captura de quadros dispositivos móveis dos usuários legítimos presentes no cenário durante a autenticação na transição.

5.3 Parâmetros e métricas

No ambiente de simulação, os parâmetros foram configurados de acordo com as características das redes e do atacante que executa a replicação dos quadros de autenticação. Os parâmetros foram obtidos de acordo com os trabalhos encontrados na literatura que tratam da autenticação nas redes heterogêneas. Nesses trabalhos, o cenário possui dispositivos com mobilidade que variam de velocidade ou permanecem estáticos e a composição das redes é formulada de forma realística representando um centro urbano ou comercial.

A Tabela 5.1 resume os valores usados na configuração das redes heterogêneas. O parâmetro da quantidade de nós na avaliação variou entre 20, 40 e 60. Os nós que compreendem os dispositivos móveis comuns possuem mobilidade. Essa mobilidade é aleatória no cenário de avaliação com velocidades entre 2m/s e 5m/s. Os nós atacantes são fixos. A posição desses nós é aleatória em relação às localizações do cenário onde existem sobreposições de redes. A comunicação dos nós legítimos considera as tecnologias com padrões 802.11 (WiFi) e *Long Term Evolution* (LTE). A simulação foi repetida 30 vezes e cada simulação teve a duração de 600 segundos. A quantidade de atacantes representa 10% da quantidade de nós da avaliação.

Parâmetros	**Valores**
Quantidade de nós	20, 40 e 60
Modelo de mobilidade	*Random Waypoint*
Velocidade dos nós	2m/s a 5m/s
Tempo de Simulação	600 s
Tecnologia	WiFi e LTE
Nós atacantes	10%

Tabela 5.1: Parâmetros de Simulação

A avaliação do serviço de autenticação do *handover* no contexto de redes heterogêneas necessita de métricas que quantificam a confidencialidade e integridade. Além disso, a avaliação deve mostrar o custo que o esquema causa no funcionamento da rede quando posto em prática. Para isso, as métricas foram escolhidas com a finalidade de demonstrar que o esquema não prejudica o desempenho da rede de maneira significativa.

Logo, as métricas para avaliar o controle de autenticação compreendem os aspectos de segurança e desempenho da rede. Os aspectos de segurança que relacionam o tipo do ataque consistem da taxa de detecção, taxa de falso positivo e taxa de falso negativo. A taxa de detecção é importante pois demonstra o quanto o esquema é eficiente em resolver o ataque de repetição e tem sido utilizado na literatura como característica fundamental de eficácia. Apesar disso, os esquemas apresentam falhas devido o ambiente sem fio, mobilidade dos usuários, interferências e outros fatores que afetar a transmissão de dados. Para quantificar essa falha várias métricas podem ser empregadas em diversos contextos. Como se trata de um serviço de segurança no acesso, a métrica que mais se adapta ao contexto apresentado neste trabalho é a taxa de falsos positivos. A taxa de falsos positivos mostra quando o esquema falhou em bloquear um ataque quando a mensagem de autenticação enviada de um dispositivo móvel para o ponto de acesso era legítima. Dessa forma, as métricas de segurança usadas são a ***Taxa de ataques de repetição prevenidos*** (T_{prev}) e a ***Taxa de falso positivos*** (T_{fa}).

A **Taxa de ataques de repetição prevenidos** T_{prev} representa os quadros repetidos descartados pelos esquemas que corresponde a razão entre o somatório de ataques prevenidos, *prev*, e a quantidade de ataques de repetição, *rep*, (Eq. 1).

$$T_{prev} = \frac{\sum prev}{rep} \quad (1)$$

A **Taxa de falso positivos** T_{fa} corresponde a quantidade de vezes que ocorreu alerta falso do ataque de repetição de identidades e é representado pelo somatório de prevenções, *prev*, pelo total de requisições de autenticação válidas *req*, (Eq. 2).

$$T_{fa} = \frac{\sum prev}{req} \quad (2)$$

As métricas de desempenho são ***Tempo médio de transmissão entre dispositivo móvel e ponto de acesso*** (T_x), ***Tempo médio de transmissão entre pontos de acesso*** (T_y), ***Tempo médio de transmissão entre ponto de acesso e autenticador*** (T_z), ***Custo computacional da inicialização*** (C_{ini}) e ***Custo computacional da autenticação*** (C_{aut}).

O **Tempo médio de transmissão entre dispositivo móvel e ponto de acesso** T_x consiste da razão entre o somatório dos tempos de transmissão e a quantidade de autenticação do dispositivo móvel *UE* e o ponto de acesso *AP*, T_{UE-AP} e a quantidade de autenticações efetuadas Q_{aut}, (Eq. 3).

$$T_x = \frac{\sum T_{UE-AP}}{Q_{aut}} \quad (3)$$

O **Tempo médio de transmissão entre pontos de acesso** T_y compreende a razão de tempo da transmissão os pontos de acesso, T_{AP-AP} e a quantidade de mensagens enviadas *msg*, (Eq. 4).

$$T_y = \frac{\sum T_{AP-AP}}{msg} \quad (4)$$

O **Tempo médio de transmissão entre pontos de acesso** T_z compreende a razão de tempo da transmissão entre o ponto de acesso, *AP*, e o autenticador *A*, T_{AP-A} em relação à quantidade de autenticações requisitadas entre eles *req*,(Eq. 5).

O **Tempo médio de transmissão entre ponto de acesso e autenticador** C_{ini} é a razão entre o tempo de todas as inicializações, T_{ini}, e a quantidade de inicializações efetuadas, Q_{ini}, (Eq. 6).

$$T_z = \frac{\sum T_{AP-A}}{req} \quad (5)$$

$$C_{ini} = \frac{\sum T_{ini}}{Q_{ini}} \quad (6)$$

O **Custo computacional da autenticação** C_{aut} representa a razão do tempo de autenticação, T_{aut}, pela quantidade de autenticações, C_{aut}, (Eq. 7). Essas métricas de desempenho consistem do tempo em milissegundos gasto para concluir as tarefas tanto da transmissão como também o tempo para executar cada fase do esquema de autenticação.

$$C_{aut} = \frac{\sum T_{aut}}{Q_{aut}} \quad (7)$$

5.4 Resultados e análise da simulação

A Figura 5.3 apresenta a variação de acurácia dos esquemas de autenticação ARARAS e UHA no tempo de 60 segundos. O ARARAS mostrou-se mais eficiente na detecção dos ataques de repetição de identidades que o concorrente UHA devido ao mescanismo de proteção. O mecanismo de proteção compreende as redes vizinhas onde a captura da mensagem da autenticação ocorre. Dessa forma, o esquema ARARAS consegue detectar as identidades repetidas de maneira mais ampla, ou seja, detectando as identidades repetidas nas redes vizinhas.

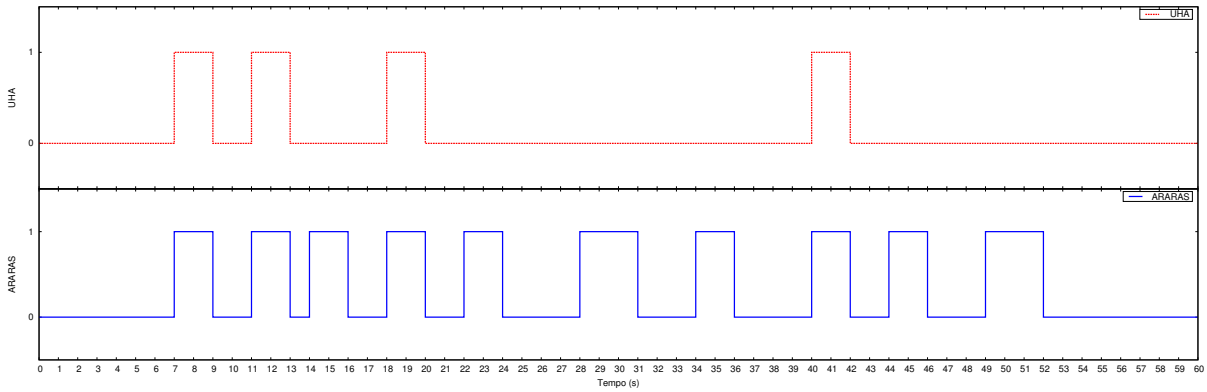


Figura 5.3: Acurácia

A Figura 5.4 representa a variação de falsos positivos dos esquemas ARARAS e UHA no tempo de 60 segundos. Assim como as Figuras 5.5 e 5.6 mostram a quantidade de falsos positivos do cenário de simulação controlado. Isso se deve pelo motivo do esquema UHA demandar mais mensagens de autenticação para que o ususário portador do dispositivo móvel

A Figura 5.7 mostra a taxa dos ataques de repetição prevenidos durante a simulação de 600 segundos. O esquema concorrente demonstra ser mais vulnerável por não possuir uma prevenção completa contra o ataque de repetição. Isso acontece em virtude da prevenção ser executada somente no mesmo ponto de acesso em que o nó legítimo está transitando. O controle de autenticação ARARAS previne o ataque de repetição de forma mais abrangente, ou seja, levando em conta todos os destinos de ataque.

A Figura 5.8 mostra a comparação da taxa de falsos positivos. O esquema UHA apesar de não levar em conta todos os casos possíveis desse ataque, possui uma taxa de falso positivo

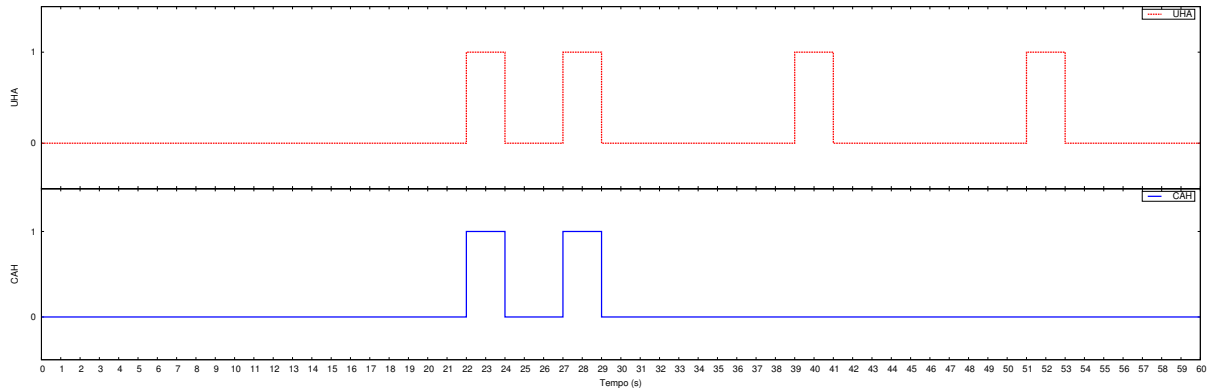


Figura 5.4: Falsos positivos

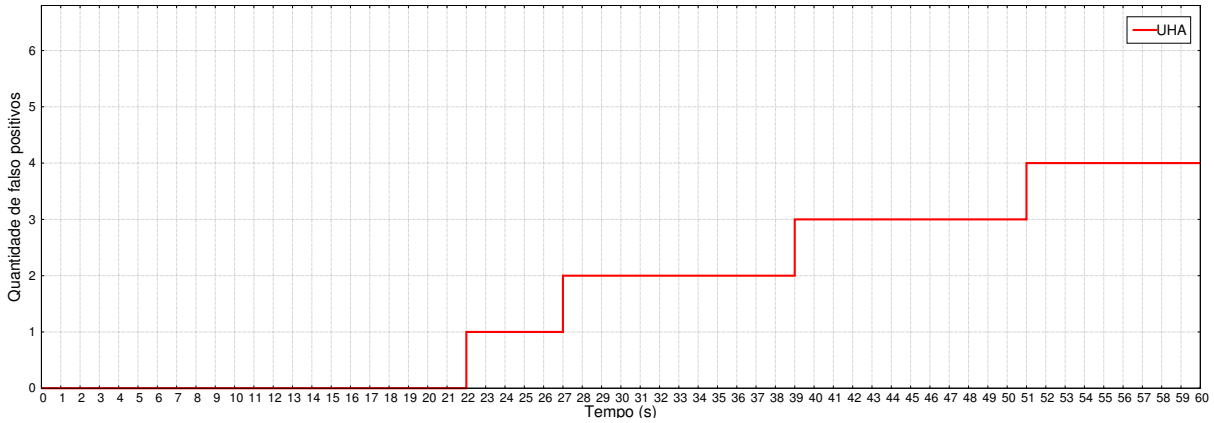


Figura 5.5: Falsos positivos do esquema UHA

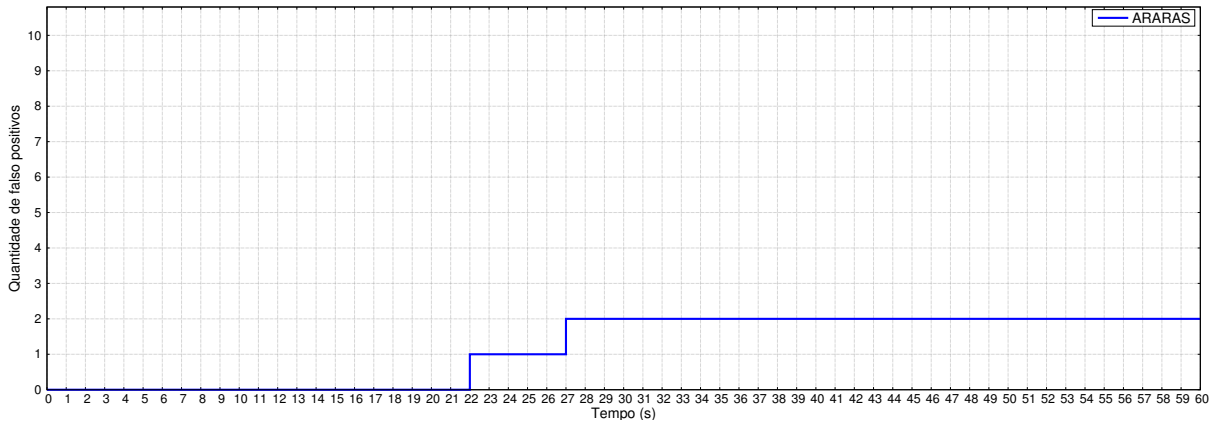


Figura 5.6: Falsos positivos do esquema ARARAS

maior que o ARARAS. Isso ocorre em virtude dos outros ataques serem prevenidos de forma mais eficaz pelo mecanismo de proteção do ARARAS que leva em consideração o tempo e quantidade de mensagem. O componente de informação desse mecanismo consegue eliminar os ataques nas redes vizinhas de forma eficaz.

A Figura 5.9 mostra o comportamento dos esquemas de autenticação quando ocorre o ataque de repetição nas redes heterogêneas. A variação da detecção do ataque de repetição no esquema ARARAS varia entre 81% à 86% enquanto o esquema UHA possui variança entre

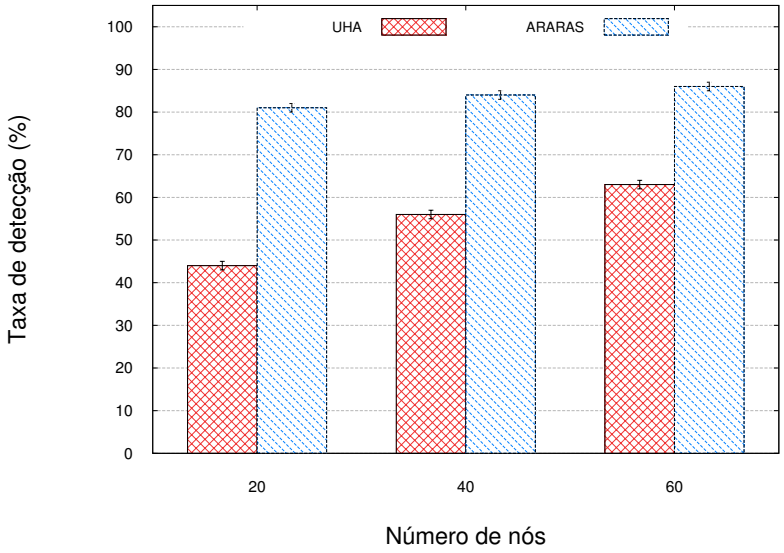


Figura 5.7: Taxa de detecção

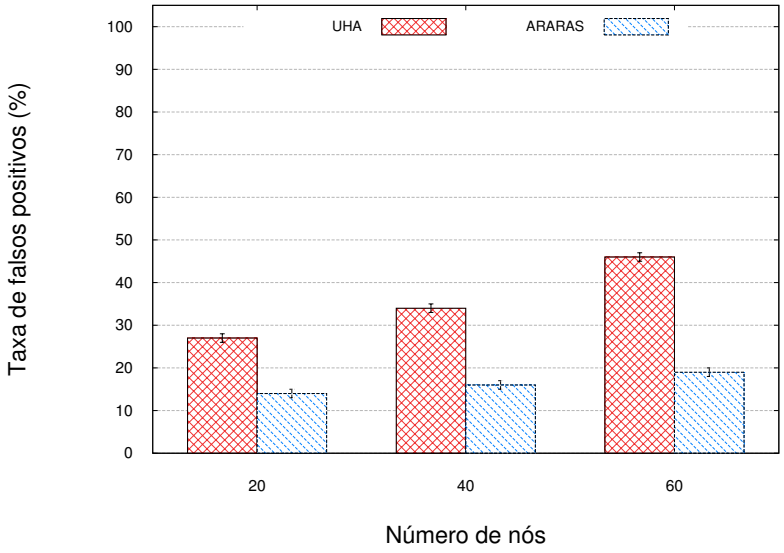


Figura 5.8: Taxa de falsos positivos

43% à 63%. O esquema ARARAS mostrou-se mais eficaz para detectar e prevenir ataques de repetição independente do tipo de tecnologia de rede empregada no cenário de simulação. Ademais, o ARARAS apresentou uma oscilação de detecção menor que o esquema concorrente devido a ocorrência da comunicação entre as entidades das redes no mecanismo de proteção.

A Figura 5.10 apresenta o comportamento dos esquemas de autenticação quando detectam ataques de repetição em mensagens de autenticação legítimas. Nesse gráfico, a variação do esquema ARARAS ficou entre 14% à 20% em falsos positivos. O UHA em contrapartida mostrou-se mais suscetível a falsos positivos, apresentando variação entre 26% à 47%. Isso ocorre devido ao esquema UHA não ter uma proteção eficaz contra o ataque de repetição quando colocado em pratica a mobilidade dos dispositivos móveis em redes com tecnologias diferentes. O ARARAS, independente da tecnologia, permite a segurança das redes a partir da fases de inicialização e autenticação juntamente com o mecanismo de proteção. No mecanismo de

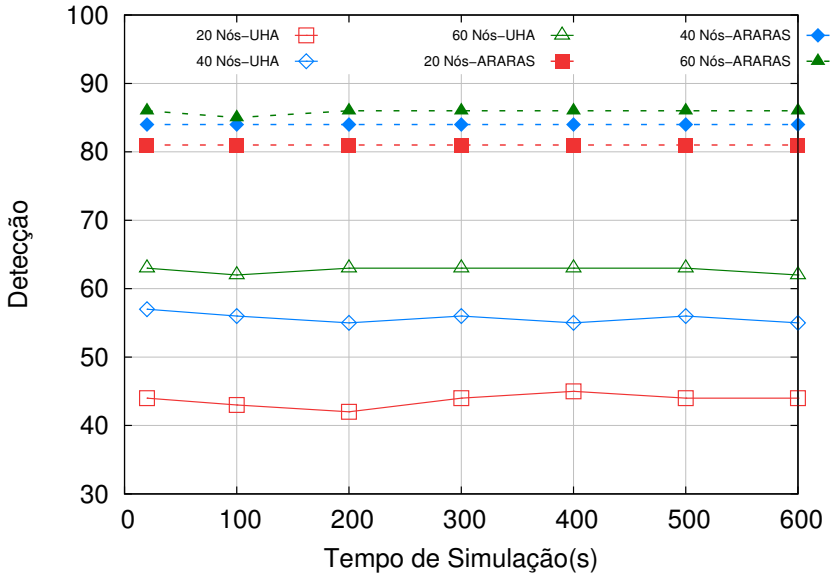


Figura 5.9: Comparativo de detecção

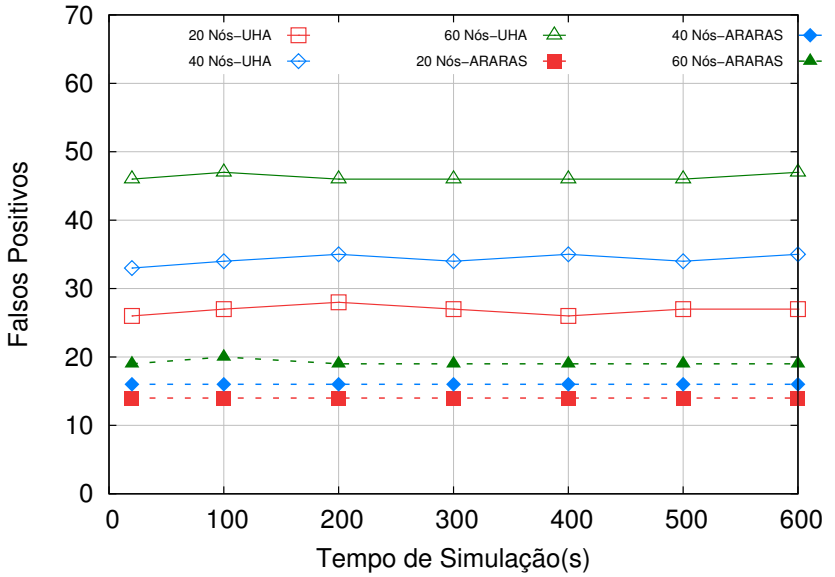


Figura 5.10: Comparativo de falsos positivos

proteção, além da verificação de tempo e quadros repetidos, a comunicação colaborativa entre as redes proveem a anulação do acesso indevido, pois as redes conseguem identificar onde está o verdadeiro dispositivo que possui a respectiva identidade e chaves replicadas por um atacante.

A Figura 5.11 apresenta a taxa total de ataques contra os tipos de tecnologias de redes. Essa diferença ocorre devido à característica de comunicação de cada tipo de rede ser diferente e pela variação de mobilidade dos dispositivos móveis. Isto proporciona aos dispositivos maliciosos uma maior capacidade para efetuar ataques. A Figura 5.12 expõe a taxa total de ataques prevenidos em cada tipo de tecnologia. A diferença de resultados compreende as características propostas por cada esquema de autenticação. O esquema UHA possui um tratamento de mensagens de autenticação efetivo em redes WiFi enquanto o esquema ARARAS impede ataques nas duas tecnologias. Isso ocorre pelo motivo da ausência de um tratamento do

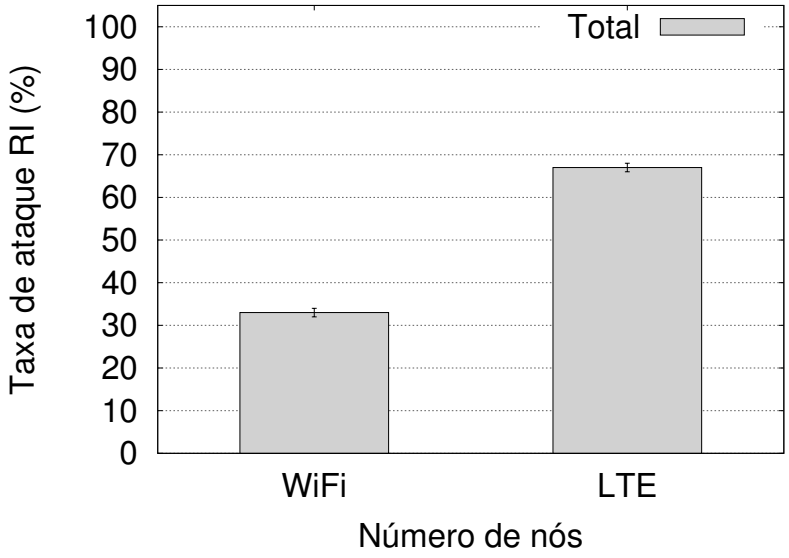


Figura 5.11: Taxa de ataques por tecnologia de rede

UHA em mensagens de ambas as tecnologias, permitindo que o atacante obtenha o acesso pela identidade na rede de maior alcance e com isso usufruir dos serviços.

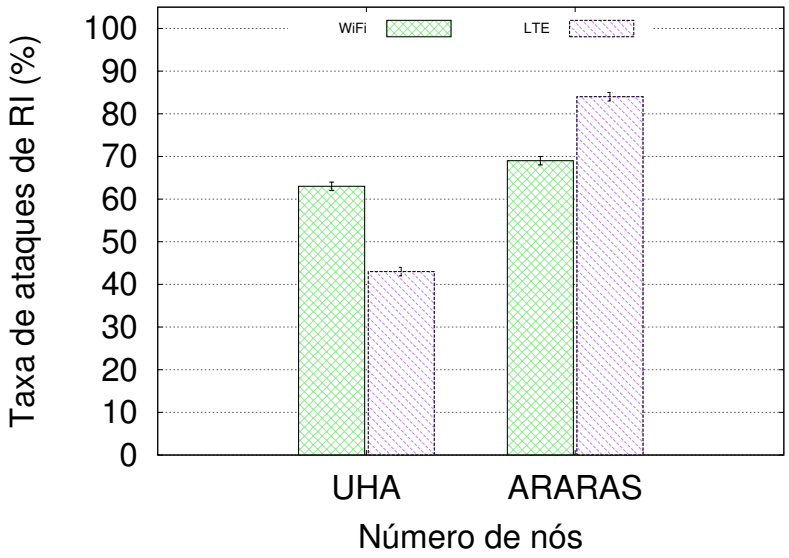


Figura 5.12: Taxa de detecção por tecnologia de rede

Para avaliar o desempenho do esquema ARARAS com o UHA, foi levada em conta a comparação da transmissão das mensagens e o custo computacional. O custo de transmissão da mensagem de autenticação consiste da comunicação entre o UE e o AP, o custo entre APs e entre o AP e o servidor de autenticação (AU), respectivamente. Dessa forma, a Tabela 5.2 mostra as despesas gerais de transmissão dos sistemas de comunicação, e representa o desempenho das comunicações entre as entidades da rede heterogênea. As comunicações consistem do dispositivo móvel e ponto de acesso (UE-AP), do ponto de acesso com ponto de acesso (AP-AP), e do ponto de acesso e autenticador central (AP-A). A diferença de tempo está na relação da comunicação

entre o dispositivo móvel e o ponto de acesso devido ao uso do pareamento que representa um método de processamento rápido para cifrar a informação.

Esquema	UE-AP	AP-AP	AP - A
UHA	4 ms	0	2 ms
ARARAS	2 ms	0	2 ms

Tabela 5.2: Comparação de transmissão

Esquema	Tempo de Inicialização	Tempo de *handover*
UHA	3 ms	4.5 ms
ARARAS	3 ms	2 ms

Tabela 5.3: Comparação de custo computacional

A Tabela 5.3 mostra uma comparação do custo computacional do esquema de autenticação UHA com o ARARAS. O pareamento obteve uma autenticação mais rápida em relação a troca de mensagens. O controle de autenticação ARARAS mostrou-se mais seguro e com melhor desempenho de comunicação em relação ao concorrente UHA. Isso se deve pelo motivo do pareamento ser realizado de forma unificada entre as redes possibilitando ao serviço de autenticação uma execução mais rápida.

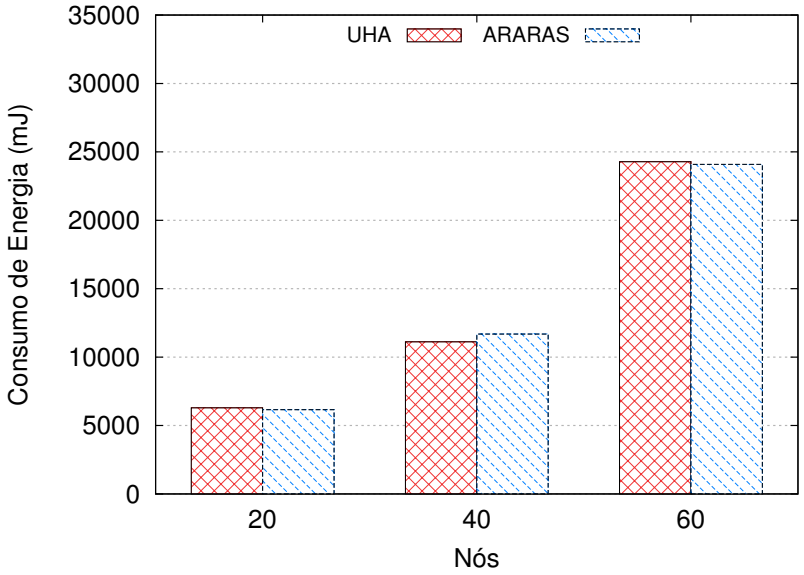


Figura 5.13: Consumo energético fase 1

O consumo energético em milijoules consiste das figuras 5.13 e 5.14. De acordo com os resultados obtidos na simulação correspondente a 5.13, o consumo energético na fase e inicialização do esquema ARARAS que corresponde a primeira autenticação do UHA possui consumo energético semelhante para as quantidades de nós presentes no ambiente. Na fase de autenticação do processo de *handover* que compreende a 5.14, o esquema ARARAS apresentou vantagens em relação ao concorrente UHA devido as diferenças entre as metodologias de criptografia empregadas em ambos os esquemas. Devido a troca de mensagens ser menor, a autenticação do ARARAS conseguiu ser menos custosa na fase de *handover* entre as redes heterogêneas.

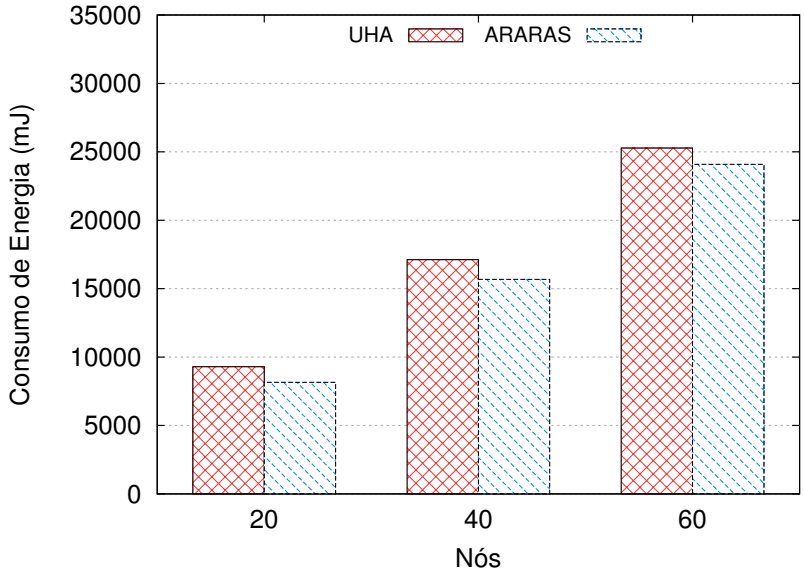


Figura 5.14: Consumo energético fase 2

5.5 Resumo

Este capítulo apresentou uma avaliação do funcionamento e do desempenho dos esquemas de autenticação ARARAS e UHA. Foram utilizadas métricas de segurança e desempenho para comparação dos resultados. As métricas de segurança foram a taxa de ataques de repetição prevenidos T_{prev} e a taxa de falso positivos T_{fa}. As métricas de desempenho foram o tempo médio de transmissão entre dispositivo móvel e ponto de acesso T_x, tempo médio de transmissão entre pontos de acesso T_y, tempo médio de transmissão entre ponto de acesso e autenticador T_z, custo computacional da inicialização C_{ini} e custo computacional da autenticação C_{aut}. Os resultados apresentaram que o esquema ARARAS foi mais eficiente para eliminar os ataques de repetição sendo superior ao UHA.

Capítulo 6

Conclusão

As Redes Heterogêneas sem fio (RHSFs) consistem de diversas redes compostas por tecnologias de comunicação diferentes que fornecem aos usuários portadores de dispositivos computacionais a continuidade da conexão e dos serviços. Ademais, essas redes possuem o suporte de alguns serviços que prestam a interoperabilidade entre as diferentes tecnologias de comunicação. Apesar disso, alguns serviços, como a autenticação, estão vulneráveis a ataques de repetiçãode identidade, afetando assim a confidencialidade e a disponibilidade do acesso às redes.

Embora vários trabalhos na literatura apresentem esquemas de autenticação com o propósito de tornar o controle de acesso mais seguro contra vários ataques em redes homogêneas e heterogêneas, eles possuem diferentes estratégias que quando levadas para o contexto de redes com tecnologias comunicação diferente se tornam inviáveis devido à limitações como quantidade de dispositivos móveis, segurança e o desempenho. Além disso, as estratégias acarretam no atraso do serviço de autenticação quando requisitado o *handover* vertical. Por se tratar de um contexto de redes heterogêneas, diversos ataques que visam obter o acesso não autorizado através da identidade são efetivos.

O esquema de autenticação ARARAS foi proposto com o objetivo de resistir ao ataque de repetição de identidades que ocorre no serviço de autenticação nas redes heterogêneas sem fio. Esse esquema consiste de duas fases para a inicialização e autenticação dos dispositivos móveis nas redes e de um mecanismo de proteção. Na fase de inicialização o dispositivo móvel executa a primeira autenticação com o autenticador global através de um canal seguro no qual garante que ataque externos não possam ser realizados. Com base na identidade do usuário, o emparelhamento bilinear, presente no autenticador de rede, gera as chaves de acesso. Na fase de autenticação, o dispositivo móvel pode efetuar uma autenticação durante o *handover* vertical de forma mais rápida decorrente da unificação do esquema de autenticação com redes de tecnologias diferentes. Para proteger essa fase de autenticação, o mecanismo de proteção da rede barra as mensagens falsas replicadas por um atacante através de métodos de análise de tempo, quantidade de mensagem e da distribuição das informações da autenticação para redes vizinhas e a rede de maior abrangência de comunicação sem fio, na qual foi realizada a inicialização.

A implementação do esquema de autenticação foi feita no simulador de redes NS3 onde foi considerado um cenário de redes heterogêneas sem fio no cenário urbano. Nessa avaliação, o ARARAS foi comparado com o esquema UHA através de métricas de segurança e desempenho. O UHA se trata de um esquema de autenticação para redes heterogêneas e foi implementado usando as mesmas características de simulação para avaliar o esquema proposto. Estes dois esquemas foram avaliados levando em conta o mesmo cenário na presença de ataques de repetição. Os resultados obtidos mostraram a eficiência e a eficácia do ARARAS na detecção

de ataques de repetição de identidade no handover vertical obtendo uma elevada taxa de detecção com um consumo razoável de energia para RHSF. Ademais, o ARARAS alcançou uma boa eficiência com baixas taxas de falsos positivos.

Em relação a comparação dos resultados com o esquema UHA, o ARARAS apresentou resultados superiores devido à forma como ele gerencia a autenticação dos dispositivos móveis e pelo mecanismo de proteção que previne o ataque em redes vizinhas. O esquema UHA demonstrou ser mais vulnerável tendo uma taxa de detecção inferior e maior índice de falso positivos. Além disso, o UHA mostrou-se ser mais efetivo em redes de padrão WiFi do que em redes LTE. A partir dos resultados obtidos, conclui-se que o ARARAS atende aos requisitos para assegurar o serviço de autenticação durante o handover vertical nas redes heterogêneas. Ele demonstrou que consegue ser eficaz contra ataques de repetição de identidade em ambas as tecnologias de redes.

6.1 Trabalhos futuros

O esquema proposto nesta dissertação pode ser avaliado sobre a perspectiva de outros ataques de autenticação como dessincronização, hijacking, injeção de códigos maliciosos, entre outros. Para expandir esse esquema, alguns módulos poderiam ser acrescentados com o objetivo de reforçar a segurança contra esses e outros ataques que prejudicam o controle de acesso de usuários na rede. Ademais, como o trabalho trata da confidencialidade e disponibilidade, outros aspectos de segurança poderiam ser considerados para a avaliação.

O crescente uso de dispositivos computacionais móveis estão crescendo a cada ano e com isso novos problemas surgirão nas novas tecnologias de redes sem fio. Como o esquema ARARAS foi avaliado considerando as tecnologias de redes WiFi e LTE, novas adaptações poderiam ser feitas para o padrão IEEE 802.11ac como também as redes 5G ou mesmo redes virtualizadas para tornar o trabalho mais completo.

Referências Bibliográficas

[1] Jeffrey G Andrews. Seven ways that hetnets are a cellular paradigm shift. *IEEE Communications Magazine*, 51(3):136–144, 2013.

[2] O. Khattab and O. Alani. Survey on media independent handover (mih) approaches in heterogeneous wireless networks. In *Proceedings of the 2013 19th European Wireless Conference (EW)*, páginas 1–5, Abril 2013.

[3] Ian F Akyildiz, Jiang Xie, and Shantidev Mohanty. A survey of mobility management in next-generation all-ip-based wireless systems. *IEEE Wireless Communications*, 11(4):16–28, 2004.

[4] S. Ranjan, N. Akhtar, M. Mehta, and A. Karandikar. User-based integrated offloading approach for 3GPP LTE-WLAN network. In *Twentieth National Conference on Communications (NCC)*, páginas 1–6, Fevereiro 2014.

[5] Kire Jakimoski and Toni Janevski. Vertical handover improvements from wlan to wman or wwan technologies. In *IEEE 11th International Conference on Telecommunication in Modern Satellite, Cable and Broadcasting Services (TELSIKS)*, volume 2, páginas 605–608, 2013.

[6] Alexander D. Kent, Lorie M. Liebrock, and Joshua C. Neil. Authentication graphs: Analyzing user behavior within an enterprise network. *Computers & Security*, 48(0):150 – 166, 2015.

[7] D. He, S. Chan, and M. Guizani. Handover authentication for mobile networks: security and efficiency aspects. *IEEE Network*, 29(3):96–103, Maio 2015.

[8] Narn-Yih Lee and Yu-Chung Chiu. Improved remote authentication scheme with smart card. *Computer Standards & Interfaces*, 27(2):177–180, 2005.

[9] Dave Cavalcanti, Dharma Agrawal, Carlos Cordeiro, Bin Xie, and Anup Kumar. Issues in integrating cellular networks wlans, and manets: a futuristic heterogeneous wireless network. *IEEE Wireless Communications*, 12(3):30–41, 2005.

[10] Jin Cao, Maode Ma, Hui Li, Yueyu Zhang, and Zhenxing Luo. A survey on security aspects for lte and lte-a networks. *IEEE Communications Surveys & Tutorials*, 16(1):283–302, 2014.

[11] R. Singh and T.P. Sharma. A sequence number based wlan authentication scheme for reducing the mic field overhead. In *Tenth International Conference on Wireless and Optical Communications Networks (WOCN)*, páginas 1–4, Julho 2013.

[12] Cédric Adjih, Daniele Raffo, and Paul Mühlethaler. Attacks against olsr: Distributed key management for security. In *2nd OLSR Interop/Workshop, Palaiseau, France*, 2005.

[13] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour. A survey of routing attacks in mobile ad hoc networks. *IEEE Wireless Communications*, 14(5):85–91, Outubro 2007.

[14] Daojing He, Chun Chen, Sammy Chan, and Jiajun Bu. Secure and efficient handover authentication based on bilinear pairing functions. *IEEE Transactions on Wireless Communications*, 11(1):48–53, 2012.

[15] Shin-Ming Cheng, Cheng-Han Ho, Shannon Chen, and Shih-Hao Chang. Distributed anonymous authentication in heterogeneous networks. In *Wireless Communications and Mobile Computing Conference (IWCMC)*, páginas 505–510, Agosto 2014.

[16] Hou Huifang, Wang Yuhua, Wang Yunxia, and Liu Guangqiang. An identity-based access authentication scheme for heterogeneous wireless network. In *5th International Conference on Wireless Communications, Networking and Mobile Computing*, páginas 1 – 4, Setembro 2009.

[17] Jin Cao, Maode Ma, and Hui Li. Unified handover authentication between heterogeneous access systems in lte networks. In *IEEE Global Communications Conference (GLOBECOM)*, páginas 5308–5313, 2012.

[18] Qin Yu, Wei Jiang, and Zhihui Xiao. 3g and wlan heterogeneous network handover based on the location information. In *Communications, Circuits and Systems (ICCCAS), 2013 International Conference on*, volume 2, páginas 50–54. IEEE, 2013.

[19] Yih-Chun Hu, A. Perrig, and D.B. Johnson. Packet leashes: a defense against wormhole attacks in wireless networks. In *Twenty-Second Annual Joint Conference of the IEEE Computer and Communications INFOCOM*, volume 3, páginas 1976–1986, Março 2003.

[20] Yueming Deng, Guojun Wang, and Jiannong Cao. Practical unified authentication for 3g-wlan interworking. *Journal of Information & Computational Science*, 9(7):9, 2012.

[21] Aleksandar Damnjanovic, Juan Montojo, Yongbin Wei, Tingfang Ji, Tao Luo, Madhavan Vajapeyam, Taesang Yoo, Osok Song, and Durga Malladi. A survey on 3gpp heterogeneous networks. *IEEE Wireless Communications*, 18(3):10–21, 2011.

[22] Peng Lin, Jin Zhang, Yanjiao Chen, and Qian Zhang. Macro-femto heterogeneous network deployment and management: from business models to technical solutions. *IEEE Wireless Communications*, 18(3):64–70, Junho 2011.

[23] D. Cavalcanti, D. Agrawal, Carlos Cordeiro, Bin Xie, and A. Kumar. Issues in integrating cellular networks wlans, and manets: a futuristic heterogeneous wireless network. *IEEE Wireless Communications*, 12(3):30–41, Junho 2005.

[24] J. Jackson Juliet Roy, V. Vaidehi, and S. Srikanth. Always best-connected qos integration model for the wlan, wimax heterogeneous network. In *First International Conference on Industrial and Information Systems*, páginas 361–366, Agosto 2006.

[25] R.H. Khan and J.Y. Khan. A heterogeneous wimax-wlan network for ami communications in the smart grid. In *IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*, páginas 710–715, Novembro 2012.

[26] K.N. Ashraf, V. Amarsinh, and D. Satish. Survey and analysis of mobility management protocols for handover in wireless network. In *IEEE 3rd International Advance Computing Conference (IACC)*, páginas 413–420, Fevereiro 2013.

[27] Arif Ahmed, Leıla Merghem Boulahia, and Dominique Gaiti. Enabling vertical handover decisions in heterogeneous wireless networks: A state-of-the-art and a classification. *IEEE Communications Surveys & Tutorials*, 16(2):776–811, 2014.

[28] P. Tinkhede and P. Ingole. Survey of handover decision for next generation. In *International Conference on Information Communication and Embedded Systems (ICICES)*, páginas 1–5, Fevereiro 2014.

[29] Nilakshee Rajule, Bhavna Ambudkar, and AP Dhande. Survey of vertical handover decision algorithms. *Inter. Journal of Innovations in Engineering and Tech*, 2(1):362–368, 2013.

[30] Johann Márquez-Barja, Carlos T Calafate, Juan-Carlos Cano, and Pietro Manzoni. An overview of vertical handover techniques: Algorithms, protocols and tools. *Computer Communications*, 34(8):985–997, 2011.

[31] Mahdi Aiash, Glenford Mapp, and Aboubaker Lasebae. A survey on authentication and key agreement protocols in heterogeneous networks. *arXiv preprint arXiv:1208.1918*, 2012.

[32] Sung Choi and D. Zage. Addressing insider threat using x201c;where you are x201d; as fourth factor authentication. In *IEEE International Carnahan Conference on Security Technology (ICCST)*, páginas 147–153, Outubro 2012.

[33] John Clark and Jeremy Jacob. A survey of authentication protocol literature: Version 1.0.

[34] Hung-Min Sun, Yao-Hsin Chen, and Yue-Hsun Lin. opass: A user authentication protocol resistant to password stealing and password reuse attacks. *IEEE Transactions on Information Forensics and Security*, 7(2):651–663, 2012.

[35] Kamlesh Gupta and Sanjay Silakari. Ecc over rsa for asymmetric encryption: A review. *IJCSI International Journal of Computer Science Issues*, 8(3), 2011.

[36] KU Wei-Chi, CHEN Chien-Ming, and LEE Hui-Lung. Cryptanalysis of a variant of peyravian-zunic's password authentication scheme. *IEICE Transactions on Communications*, 86(5):1682–1684, 2003.

[37] Shi Zhong, Taghi M Khoshgoftaar, and Shyarn V Nath. A clustering approach to wireless network intrusion detection. In *17th IEEE International Conference on Tools with Artificial Intelligence (ICTAI)*, páginas 7 pp.–196, 2005.

[38] Jane Zhen and Sampalli Srinivas. Preventing replay attacks for secure routing in ad hoc networks. In *Ad-Hoc, Mobile, and Wireless Networks*, páginas 140–150. Springer, 2003.

[39] Manik Lal Das, Ashutosh Saxena, and Ved P Gulati. A dynamic id-based remote user authentication scheme. *IEEE Transactions on Consumer Electronics*, 50(2):629–631, 2004.

[40] Tao Feng and Jian Jiao. WAPI secure access authentication scheme for heterogeneous networks based on identity-based cryptograph. In *8th IEEE International Conference on Computing Technology and Information Management (ICCM)*, volume 1, páginas 130–135, 2012.

[41] Xiaowei Li, Yuqing Zhang, Xuefeng Liu, Jin Cao, and Qianqian Zhao. A lightweight roaming authentication protocol for anonymous wireless communication. In*IEEE Global Communications Conference (GLOBECOM)*, páginas 1029–1034, 2012.

[42] Anmin Fu, Gongxuan Zhang, Yuqing Zhang, and Zhenchao Zhu. Ghap: An efficient group-based handover authentication mechanism for ieee 802.16 m networks. *Wireless personal communications*, 70(4):1793–1810, 2013.

[43] Anmin Fu, Shaohua Lan, Bo Huang, Zhenchao Zhu, and Yuqing Zhang. A novel group-based handover authentication scheme with privacy preservation for mobile wimax networks. *IEEE Communications Letters*, 16(11):1744–1747, 2012.

[44] Thuy Ngoc Nguyen and Maode Ma. An pre-authentication protocol with symmetric keys for secure handover in mobile wimax networks. In *IEEE International Conference on Communications (ICC)*, páginas 863–867, 2012.

[45] Jaeduck Choi and Souhwan Jung. A handover authentication using credentials based on chameleon hashing. *IEEE Communications Letters*, 14(1):54–56, 2010.

[46] Anmin Fu, Yuqing Zhang, Zhenchao Zhu, and Xuefeng Liu. A fast handover authentication mechanism based on ticket for ieee 802.16 m. *IEEE Communications Letters*, 14(12):1134–1136, 2010.

[47] Chen Lyu, Dawu Gu, Yunze Zeng, and Prasant Mohapatra. Pba: Prediction-based authentication for vehicle-to-vehicle communications. *IEEE Transactions on Dependable and Secure Computing*, 13(1):71–83, 2016.

[48] Manali D Shah, Shrenik N Gala, and Narendra M Shekokar. Lightweight authentication protocol used in wireless sensor network. In *IEEE International Conference on Circuits, Systems, Communication and Information Technology Applications (CSCITA)*, páginas 138–143, 2014.

[49] Jin Cao, Maode Ma, and Hui Li. Unified handover authentication between heterogeneous access systems in lte networks. In *IEEE Global Communications Conference (GLOBECOM)*, páginas 5308–5313, 2012.

[50] R.W. Heath, M. Kountouris, and Tianyang Bai. Modeling heterogeneous network interference using poisson point processes. *IEEE Transactions on Signal Processing*, 61(16):4114–4126, Agosto 2013.

[51] Jeffrey Walton. *Data Security with Crypto++*. O'Reilly Media, Inc., 2012.

ANEXO

Este anexo descreve uma avaliação da segurança e do desempenho do esquema de autenticação UHA (*Unified Handover Authentication*) . O esquema foi escolhido por se adequar as características das redes heterogêneas, como a presença de redes sobrepostas e a necessidade da execução da transição de conexão durante a mobilidade do usuário. O UHA foi implementado no simulador de redes NS3 na versão 3.24.1. Na avaliação, este esquema foi avaliado considerando o ataque de repetição de identidades.

Avaliação

O cenário definido para a avaliação compreende um ambiente equivalente a um centro urbano. Neste cenário, os nós da rede correspondem aos dispositivos móveis dos usuários que representam os aparelhos de telefonia como smartphone. Estes nós se autenticam nas redes heterogêneas e possuem a mobilidade. Desta forma, o serviço de autenticação é requisitado para a tranferência de conexão.

No ambiente de simulação, os parâmetros foram configurados de acordo com as características das redes e do atacante que executa a replicação dos quadros de autenticação. Os parâmetros foram obtidos de acordo com os trabalhos encontrados na literatura que tratam da autenticação nas redes heterogêneas. Nestes trabalhos, o cenário possui dispositivos com mobilidade que variam de velocidade ou permanecem estáticos e a composição das redes é formulada de forma realística representando um centro urbano ou comercial.

Os parâmetros de simulação usados na configuração da rede IoT consideram a quantidade de nós variando entre 20, 40, e 60. Estes nós podem ser móveis ou fixos, onde os fixos compreendem 25% do total de nós. Eles também emitem a força do sinal recebido (RSS) por até 100 segundos (s) e se deslocam na rede através do modelo de mobilidade aleatório com velocidades entre 0.2m/s a 2m/s. A disseminação de conteúdo realizada pelos nós emprega o padrão 802.15.4. A simulação foi repetida 30 vezes com o intervalo de confiança de 95%, e cada simulação durou 600 segundos. Nos parâmetros do ataque Sybil, o número de atacantes foi fixada em 10% do total dos nós, e o comportamento em conluio solicita associação à rede com até cinco identidades por ataque.

O parâmetro da quantidade de nós na avaliação variou entre 20, 40 e 60. Os nós que compreendem os dispositivos móveis comum possuem mobilidade. Esta mobilidade é aleatória no cenário de avaliação com velocidades entre 2m/s e 5m/s. Os nós atacantes são fixos. A posição destes nós é aleatória em relação as localizações do cenário onde existem sobreposições de redes. A comunicação dos nós legítimos considera as tecnologias com padrões 802.11 (WIFI) e Long Term Evolution (LTE). A simulação foi repetida 30 vezes e cada simulação teve a duração de 600 segundos. A quantidade de atacantes representa 10% da quantidade de nós da avaliação.

As métricas empregadas na avaliação do esquema de autenticação UHA estão organizadas em segurança e desempenho. Desta forma, as métricas de segurança usadas são a ***Taxa de ataques de repetição prevenidos*** (T_{prev}) e a ***Taxa de falso positivos*** (T_{fa}). As métricas de

desempenho são ***Tempo médio de transmissão entre dispositivo móvel e ponto de acesso*** (T_x), ***Tempo médio de transmissão entre pontos de acesso*** (T_y), ***Tempo médio de transmissão entre ponto de acesso e autenticador*** (T_z), ***Custo computacional da inicialização*** (C_{ini}) e ***Custo computacional da autenticação*** (C_{aut}).

Resultados obtidos

Esta subseção descreve os resultados da segurança e desempenho do UHA. A Figura 1 mostra a taxa dos ataques de repetição prevenidos durante a simulação de 600 segundos. O esquema UHA demonstra ser mais vulnerável por não possuir uma prevenção completa contra o ataque de repetição. Isto acontece em virtude da prevenção ser executada somente no mesmo ponto de acesso em que o nó legítimo está transitando.

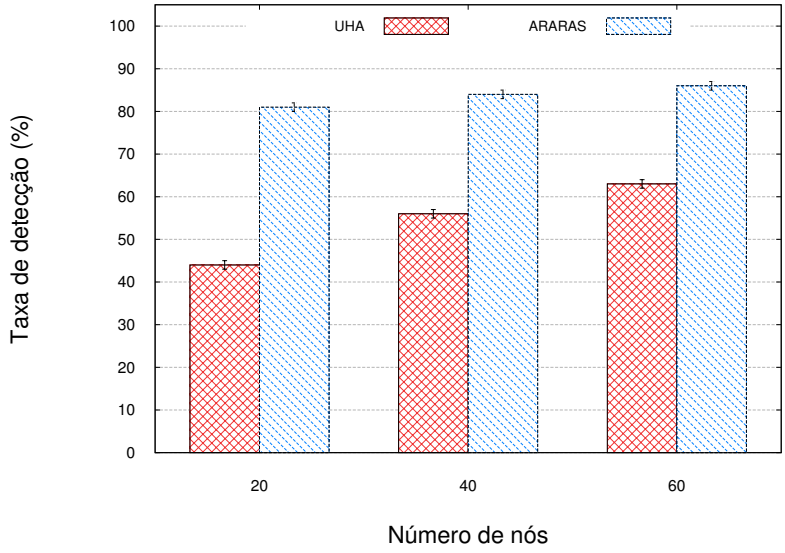


Figura 1: Taxa de detecção

A Figura 2 mostra a comparação da taxa de falsos positivos. O esquema UHA não considera todos os casos possíveis do ataque de repetição de identidade, logo, possui uma taxa de falso positivo maior. A Figura 3 mostra o comportamento dos esquemas de autenticação quando ocorre o ataque de repetição nas redes heterogêneas. O esquema UHA obteve uma variança entre 43% à 63%.

A Figura 4 apresenta o comportamento dos esquemas de autenticação quando detectam ataques de repetição em mensagens de autenticação legítimas. O UHA mostrou-se mais suscetível a falsos positivos, apresentando variação entre 26% à 47%. Isto ocorre devido ao esquema UHA não ter uma proteção eficaz contra o ataque de repetição quando colocado em pratica a mobilidade dos dispositivos móveis em redes com tecnologias diferentes.

A Figura 5 apresenta a taxa total de ataques contra os tipos de tecnologias de redes. Esta diferença ocorre devido à característica de comunicação de cada tipo de rede ser diferente e pela variação de mobilidade dos dispositivos móveis. Isto proporciona aos dispositivos maliciosos uma maior capacidade para efetuar ataques. O gráfico 6 expõe a taxa total de ataques prevenidos em cada tipo de tecnologia. A diferença de resultados compreende as características propostas por cada esquema de autenticação. O esquema UHA possui um tratamento de mensagens de autenticação efetivo em redes WiFi.

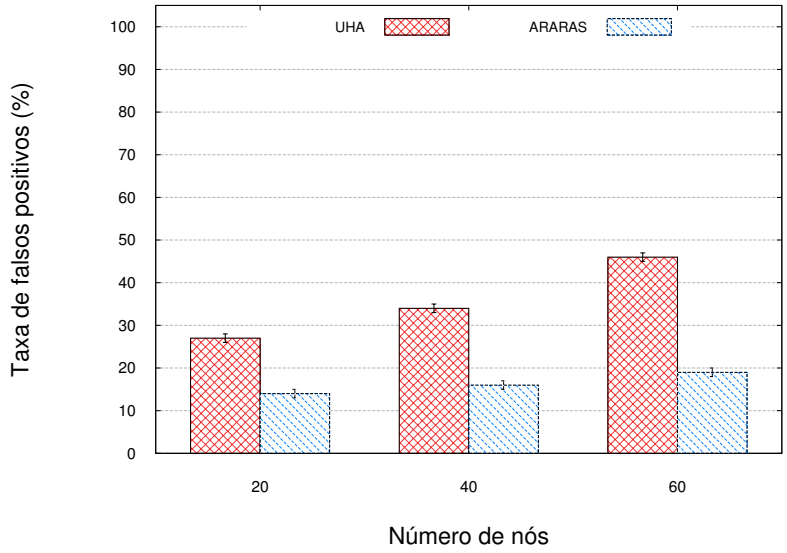


Figura 2: Taxa de falsos positivos

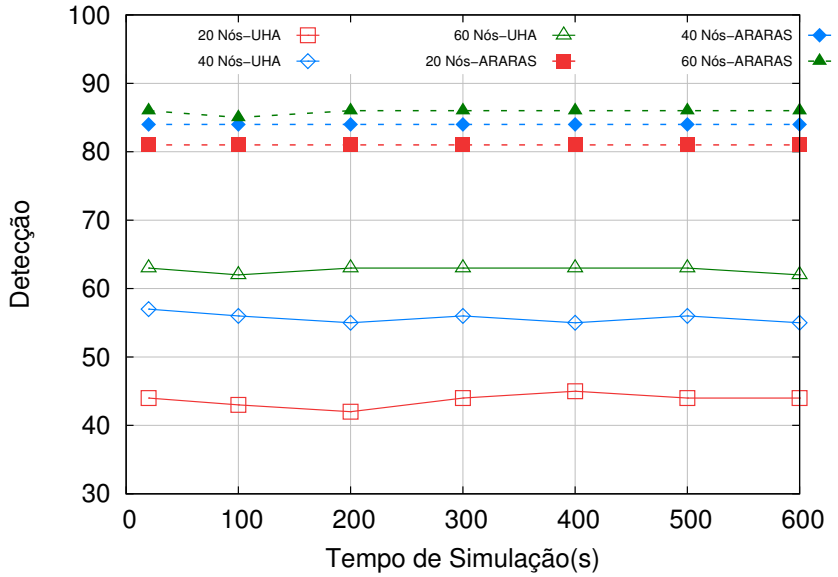


Figura 3: Comparativo de detecção

A avaliação do desempenho do esquema UHA considerou a comparação da transmissão das mensagens e o custo computacional. O custo de transmissão da mensagem de autenticação consiste da comunicação entre o UE e o AP, o custo entre APs e entre o AP e o servidor de autenticação. A Tabela 1 mostra as despesas gerais de transmissão dos sistemas de comunicação, e representa o desempenho das comunicações entre as entidades da rede heterogênea. As comunicações consistem do dispositivo móvel e ponto de acesso, do ponto de acesso com ponto de acesso, e do ponto de acesso e autenticador central. A diferença de tempo está na relação da comunicação entre o dispositivo móvel e o ponto de acesso devido ao uso do pareamento que representa um método de processamento rápido para cifrar a informação.

A Tabela 2 mostra uma comparação do custo computacional do esquema de autenticação UHA. O pareamento obteve uma autenticação mais rápida em relação a troca de mensagens.

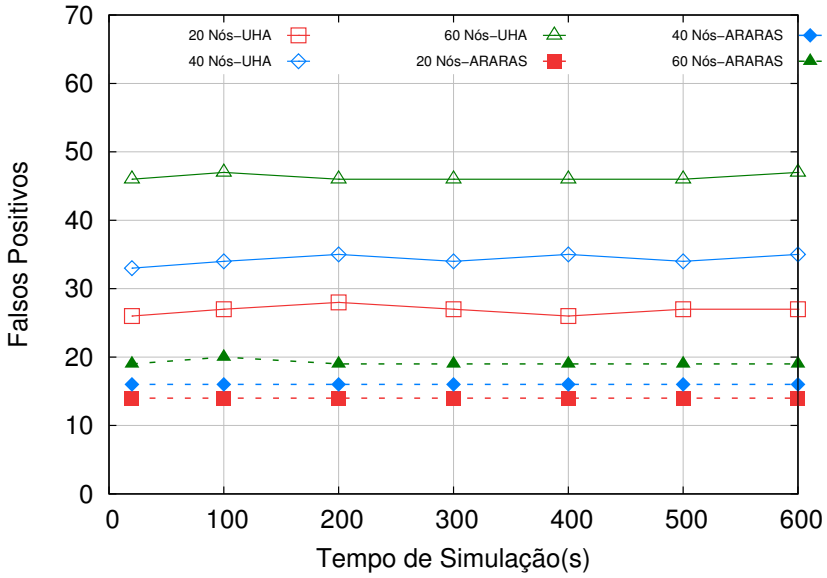


Figura 4: Comparativo de falsos positivos

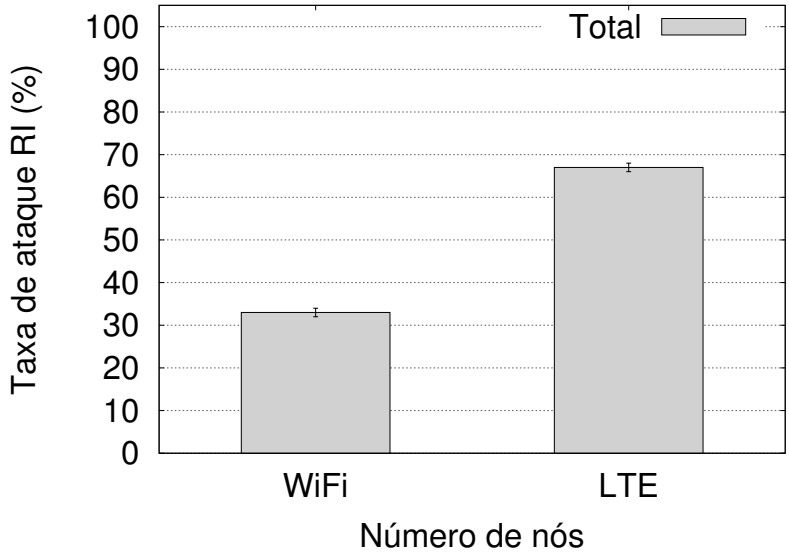


Figura 5: Taxa de ataques por tecnologia de rede

Esquema	UE-AP	AP-AP	AP - A
UHA	4 ms	0	2 ms
ARARAS	2 ms	0	2 ms

Tabela 1: Comparação de transmissão

Esquema	Tempo de Inicialização	Tempo de *handover*
UHA	3 ms	4.5 ms
ARARAS	3 ms	2 ms

Tabela 2: Comparação de custo computacional

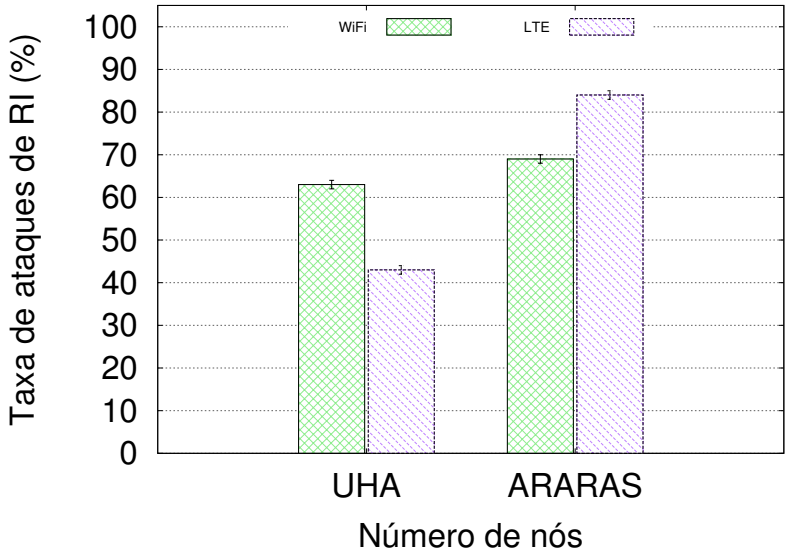


Figura 6: Taxa de detecção por tecnologia de rede

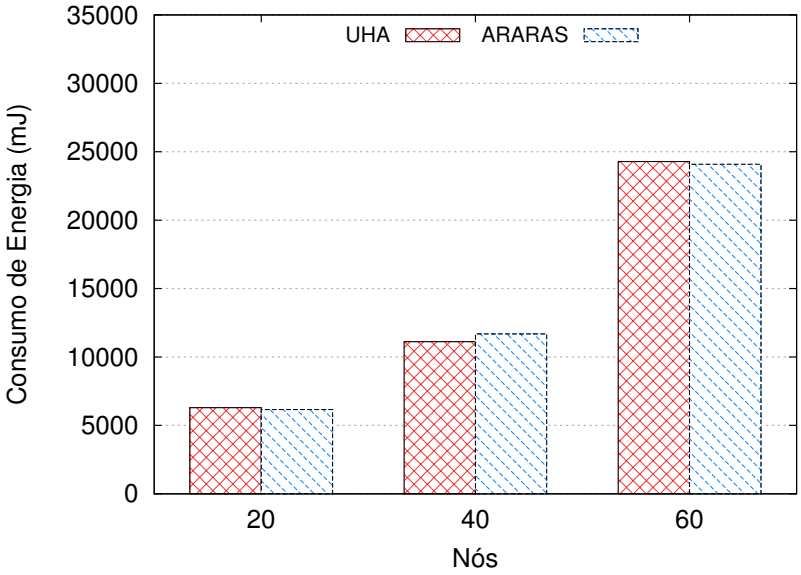


Figura 7: Consumo energético fase 1

O esquema UHA mostrou-se menos eficiente por trocar mais mensagens de autenticação para conexão de um dispositivo móvel nas redes heterogêneas.

O consumo energético em milijoules consiste das figuras 7 e 8. De acordo com os resultados obtidos na simulação correspondente a 7, o consumo energético na fase e inicialização do esquema UHA possui consumo energético semelhante ao ARARAS. Na fase de autenticação do processo de handover que compreende a 8, o esquema UHA mostrou-se inferior ao esquema ARARAS devido a maior troca de mensagens de autenticação para executar a tranferência de conexão dos dispositivos móveis e com isso maior atraso nos serviços.

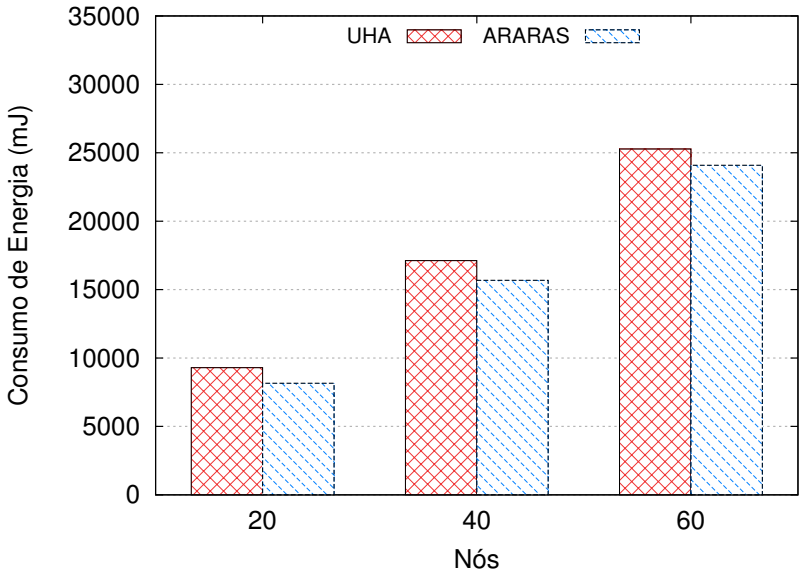


Figura 8: Consumo energético fase 2